Extreme Campus Controller User Guide

Version 5.16.03

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

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

Table of Contents

Preface

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
⚠	Caution	Risk of personal injury, system damage, or loss of data
⚠	Warning	Risk of severe personal injury

Table 2: Text

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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and software compatibility for Extreme Networks products

Extreme Optics Compatibility

Other resources such as white papers, data sheets, and case studies

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

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

Welcome to Extreme Campus Controller

ExtremeCloud Appliance has been branded Extreme Campus Controller. Extreme Campus Controller supports Campus/Centralized sites only. Support for Distributed sites remains in ExtremeCloud Appliance v4.76.02 and later and in ExtremeCloud™ IQ.

Extreme Campus Controller 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. Extreme Campus Controller offers the following features:

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

> **Note**
> Extreme Campus Controller supports Campus/Centralized sites only. During system upgrade to Extreme Campus Controller, the upgrade process checks for Distributed sites. If Distributed sites are part of the instance configuration, the upgrade process will abort and log the following:
>
> - <date> ERROR: Upgrade aborted due to the presence of a Distributed site
> - <date> ERROR: System upgrade failed
>
> After the upgrade process aborts, the system is retained at its current revision. The configuration state is not affected. Support for Distributed sites remains in ExtremeCloud Appliance v4.76.02 and later.

The Appliance

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

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

Extreme Campus Controller supports the use of both a virtual appliance and a physical appliance.

Related Topics

Appliance Product Family on page 12

Appliance Product Family

Extreme Campus Controller supports the following virtual appliances:
- **VMWare**:
  - VE6120
  - VE6125
- **Microsoft Hyper-V**
  - VE6120H

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 by Extreme Campus Controller:
- AP310i/e
- AP360i/e
- AP410i/e
- AP460i/e

- AP505i
- AP510i/e
- AP560i/h
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

The Extreme Networks® Defender Adapter SA201 is supported.

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

For a site using AP39xx, and AP3xx, AP4xx, and AP5xx, a UDP-based protocol enables communication between an AP and Extreme Campus Controller. The UDP-based protocol encapsulates IP traffic from the AP and directs it to the appliance. The appliance decapsulates the packets and encrypts (IPSec) [Default AP and appliance communication] and routes them to the appropriate destinations, while managing sessions and applying roles.

AP Client Bridge

AP Client Bridge topology extends a wired LAN using a wireless network. The Client Bridge can be used to tunnel network traffic to Extreme Campus Controller, enabling connectivity for wired devices that are moved around a facility. For example, a medical device that is moved between rooms can maintain connectivity to Extreme Campus Controller through an AP radio configured as the uplink. The medical device moves with the Client Bridge AP, the two devices can be connected through the GE2 wired port or through a wireless connection.

The deployment includes one or more infrastructure APs. After provisioning, the Client AP connects to normal infrastructure services. The infrastructure AP is essentially any AP deployed for standard service offering. The infrastructure APs communicate with the Extreme Campus Controller supporting the usual traffic flow. The Client Bridge AP roams like a wireless client, supporting background scanning to determine available infrastructure APs, Fast Roaming (11r), and Fast Client Handover to the infrastructure AP. The Client Bridge AP associates on the infrastructure AP SSID (using network credentials) establishing a Client Bridge link with the infrastructure. Manage the Client Bridge AP and its end-system clients from Extreme Campus Controller. Client statistics that are tunneled through the Client Bridge are visible from the Extreme Campus Controller Dashboard.

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

Define Client Bridge from the **Radios** tab within the configuration Profile. Only one radio can be configured as a Client Bridge. This can be either radio. Regardless of which radio is configured as the Client Bridge, both radios will continue to provide service. All ExtremeWireless 11ax APs are supported,

provided that the AP operational mode is configured for a Centralized site. Both the Client Bridge AP and the infrastructure AP must be an 11ax AP model: AP3xx, AP4xx, and AP5xx.

> **Note**
> AP39xx access points are not supported.

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

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

> **Note**
> ExtremeWireless Wi-Fi 6 access points do not provide POE to connected clients.

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

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

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

Related Topics

Managing Client Bridge in Extreme Campus Controller

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

All columns on the list screens are not displayed by default. See Configuring Column Display on page 24 to customize your column layout.

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

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

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

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

Related Topics

Configuring Column Display on page 24

AP Client Bridge on page 13

Configure Client Bridge on Extreme Campus Controller on page 101

Cloud Visibility

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

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

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

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

- An ExtremeCloud™ IQ account
- Extreme Campus Controller must be onboarded through ExtremeCloud IQ.
- Extreme Campus Controller requires internet connectivity and a Domain Name Server (DNS) configuration.

The following AP models support Cloud Visibility:

- AP3xx, AP4xx, and AP5xx
- AP39xx

- SA201 Defender Adapter

> **Note**
> Reporting of metrics for managed switches is not supported.

Related Topics

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 Extreme Campus Controller data model, the site runs Sessions Manager and RF Manager functions for all RF Domains in the site. Define the licensing domain for the site by selecting the **Country** option.

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

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

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

A site also includes the following:

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

Related Topics

Centralized Site

A Centralized configuration uses ExtremeWireless AP models AP39xx, AP3xx, AP4xx, and AP5xx. Each Wireless AP opens an IPSec tunnel to Extreme Campus Controller, and the Session Manager and RF Management policy run on Extreme Campus Controller.

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

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

The following AP models can be deployed in a Centralized site:
- AP310i/e
- AP360i/e
- AP410i/e
- AP460i/e
- AP505i
- AP510i/e
- AP560i/h
- 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.

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

Related Topics

Profiles

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

Profiles are used to configure APs and individual radios. The available configuration options depend on the AP model. For a full list of configuration settings, see Table 25 on page 96.

Figure 1 illustrates multiple sites composed of one or more device groups, sharing a configuration Profile, and a separate device group using a different Profile. The Profile can be shared across sites and device groups or not. The device group is composed of APs with the same model, configuration Profile, and RF Management profile.
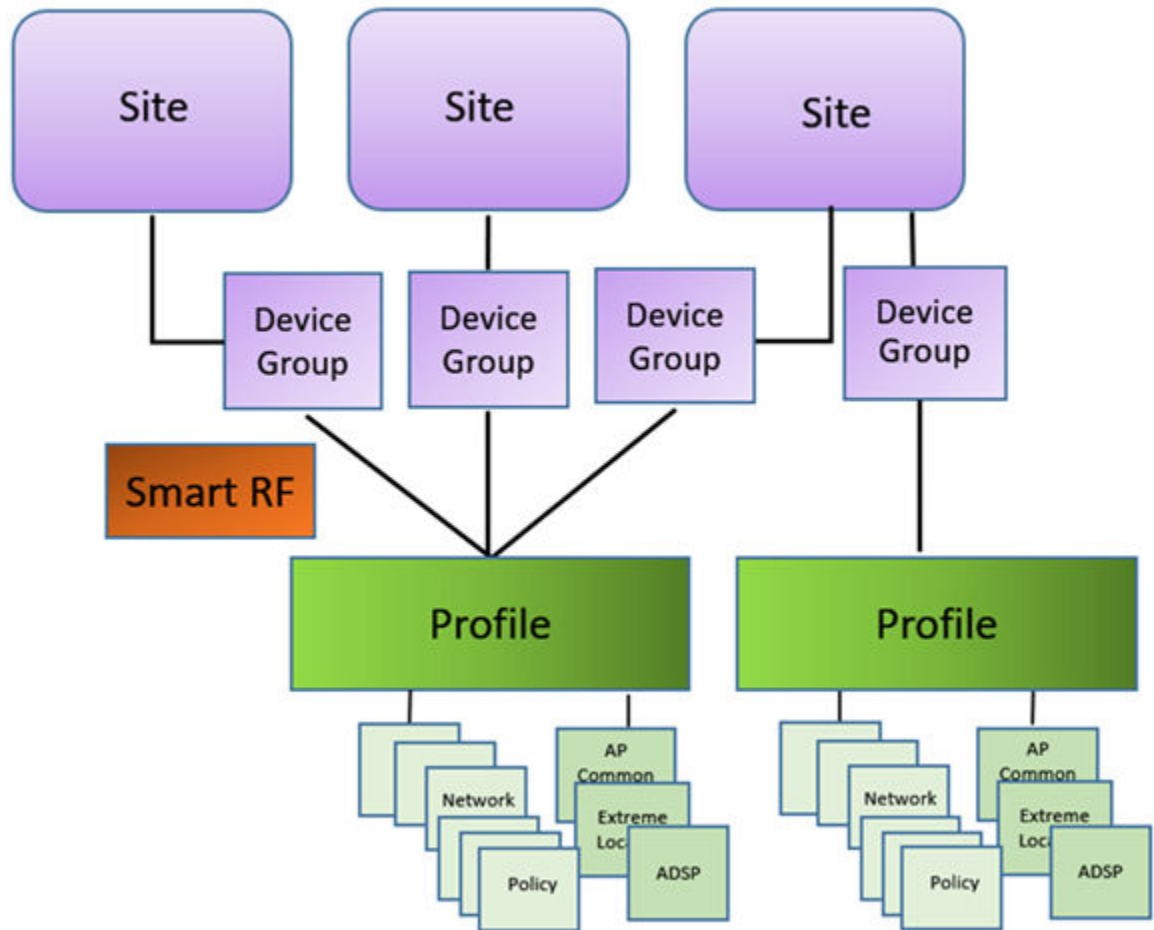
Figure 1: Site Data Model

Related Topics

Add or Edit a Configuration Profile on page 95

RF Management

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

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

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

Real-time network monitoring allows RF Management to provide self-healing functions, providing automatic mitigation from potentially problematic events such as radio interference, non-Wi-Fi

interference (noise), external Wi-Fi interference, coverage holes, and radio failures. Self-healing is used to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which would otherwise require manual reconfiguration to resolve.

Related Topics

> Configuring RF Management on page 128
>
> Configuring ACS RF Policy on page 132
>
> Configuring Smart RF Policy on page 133
>
> Smart RF Widgets on page 69

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 ▭ to display the floor plan **View**.

Related Topics

> Site Parameters on page 92
>
> Configuring a Floor Plan on page 138
>
> Floor Plan View on page 39
>
> Positioning Profile Settings on page 120

Position Aware Services

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

The Positioning Engine determines location based on measured Received Signal Strength (RSS) of the client stations at the AP. The location algorithm uses RF fingerprinting based on a Path Loss model and determines location by triangulating RSS reported from one or more APs.

Client Location Tracking is supported on AP39xx, AP3xx, AP4xx, and AP5xx. 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 Extreme Campus Controller model limit of associated clients.
- Un-Associated User. An unassociated user is a client that is not authenticated but is in the designated area. Positioning Engine can track these clients.

Related Topics

Positioning Profile Settings on page 120
Position Aware Deployment on page 21
ExtremeLocation Profile Settings on page 114

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 2: Recommended AP Placement

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

Related Topics

Position Aware Services on page 20
Positioning Heatmaps on page 49
Placing Devices on page 145

Floor Plan Limits

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

Table 4 outlines the floor plan limits for each type of Extreme Campus Controller.

Table 4: Floor Plan Limit per Appliance

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

> **Note**
> There is a file size limit for Ekahau model files:
> - 46 MB uncompressed SVG files on physical appliances:
>   - E1120
>   - E2120
>   - E3120
> - 18 MB uncompressed SVG files on virtual appliances:
>   - VE6120
>   - VE6125
>   - VE6120H
>
> Files larger than these limits will not import on the listed appliances. Consider converting large SVG files to PNG prior to import.

Related Topics

Floor Plans on page 20

Navigate the User Interface

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

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

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

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

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

Extreme Campus Controller offers the following workbenches:

Dashboard

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

Monitor

Monitor the following network components:

- Sites
- Devices
- Networks
- Clients
- Policy

Configure

Set up the following network components:

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

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.

Extreme Campus Controller offers a context-sensitive Online Help system. Select the drop-down **admin** menu on any page to access the topic-based Help System.
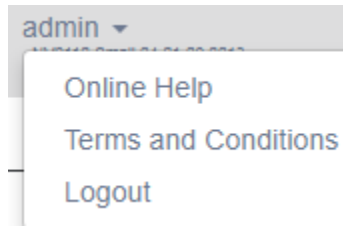
Figure 3: Extreme Campus Controller admin menu

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

The Online Help file organization corresponds to the workbench structure of Extreme Campus Controller. 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 Extreme Campus Controller offers a search facility so you can easily find what you are looking for based on specific criteria. Regular expression search, including wild cards is not supported.

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

Related Topics

Query Builder on page 52

Configuring Column Display

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

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

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

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 Extreme Campus Controller is installed.

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

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

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.

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

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.
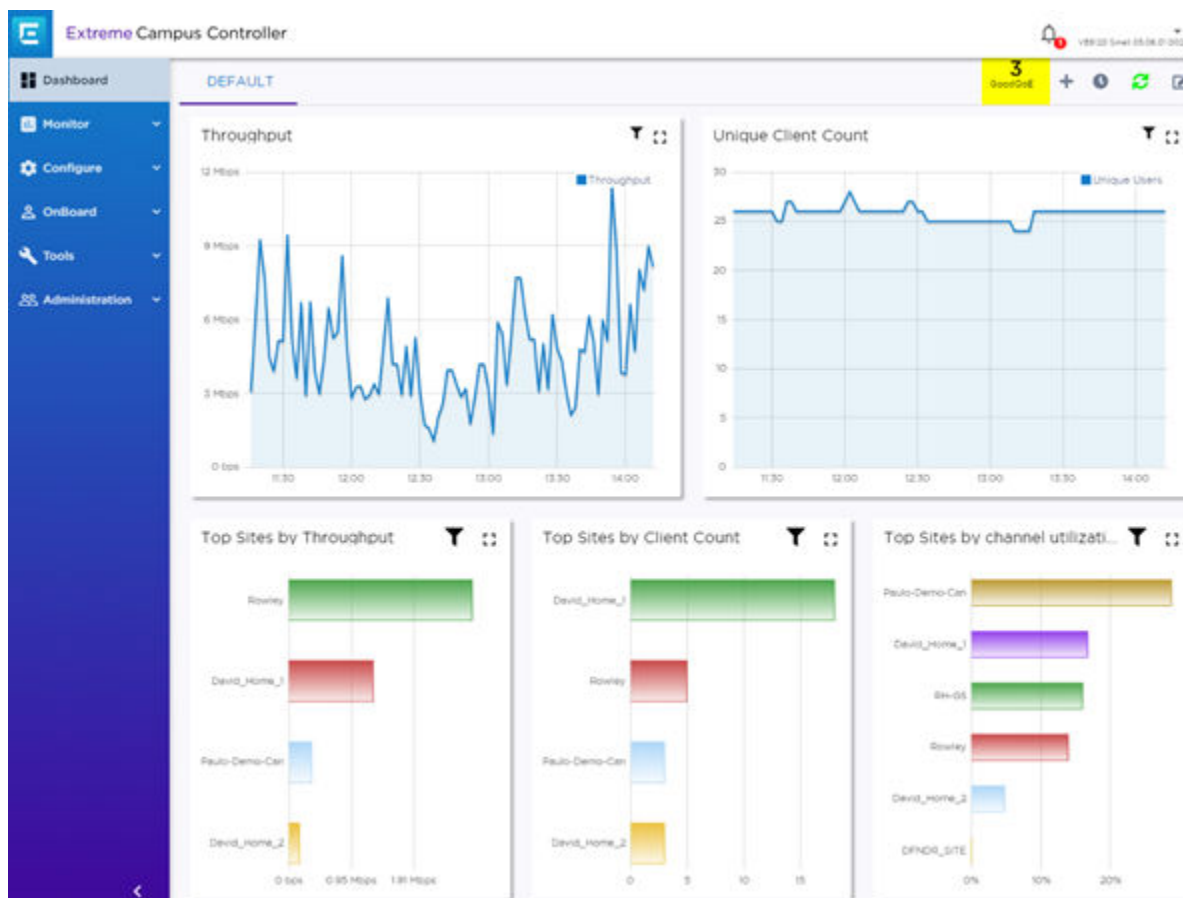
Figure 4: Main Dashboard

Related Topics

Availability Link Status on page 30
System Health Best Practice Widget on page 30

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.
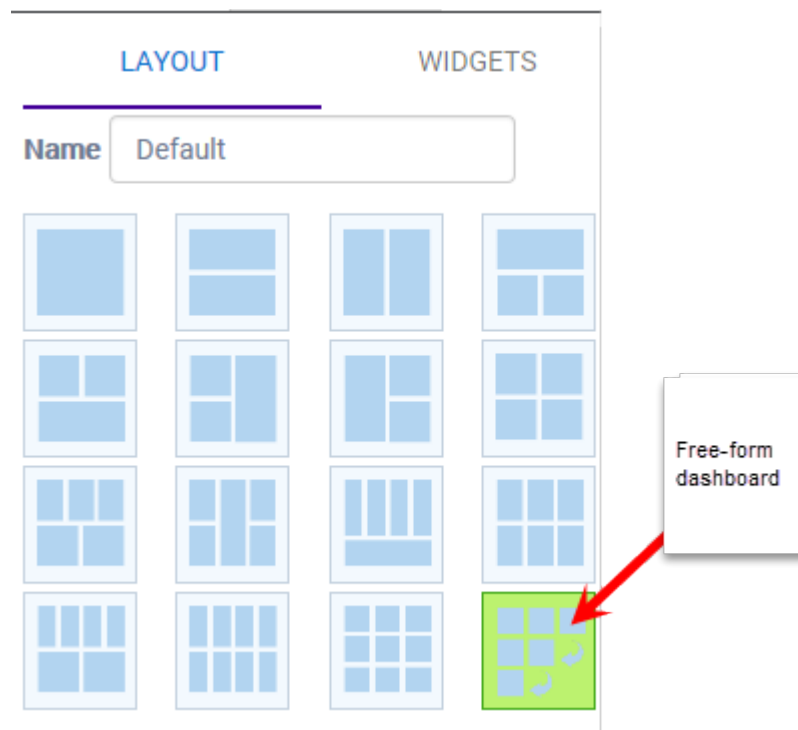
Figure 5: Widget Layout Options

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.
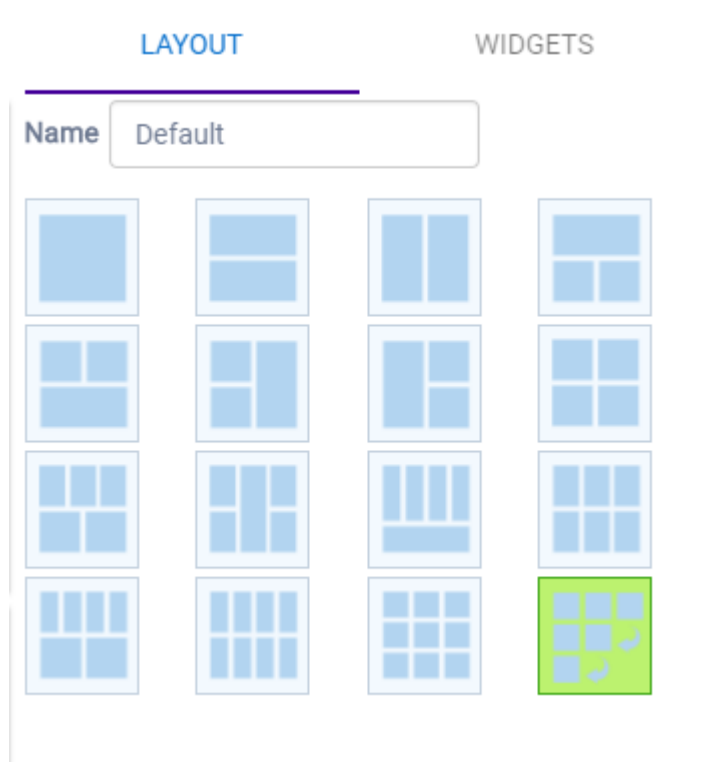
Figure 6: Dashboard - Edit Mode

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

NEW! System Health Best Practice Widget

The Extreme Campus Controller Overview dashboard offers a System Health widget that provides best practice information for your Extreme Campus Controller configuration. The System Health widget is part of the Extreme Campus Controller default dashboard. You can also find it under the System Widgets.

To access the System Health widget:

1. Go to **Dashboard**.
2. Select ✏, then **Widgets**.
3. Select the plus sign next to **System** to expand.
4. Drag the **System Health** widget onto the dashboard.
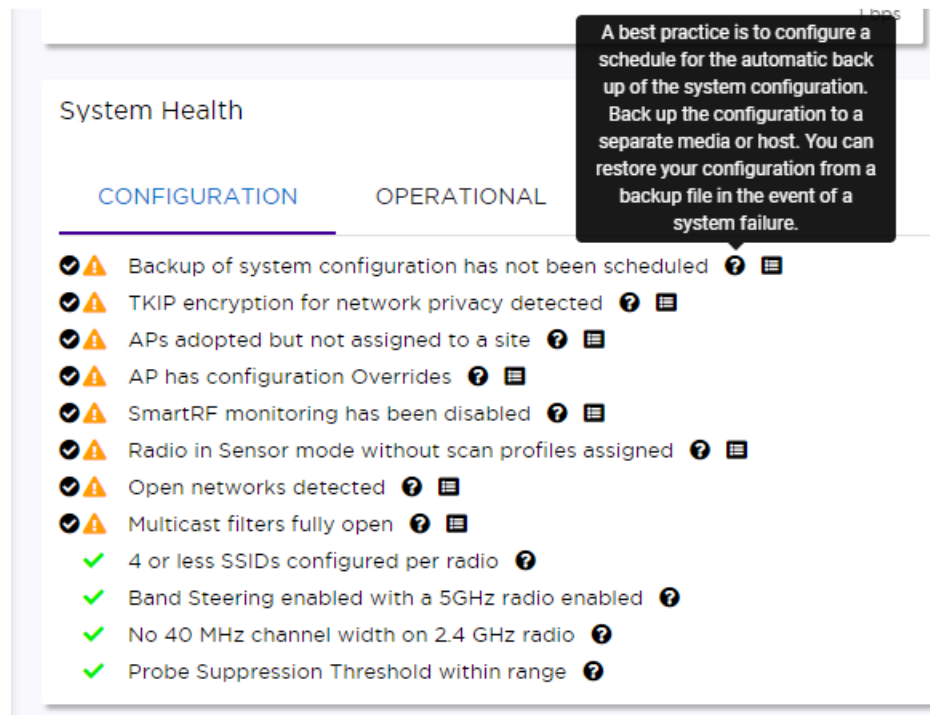
Figure 7: System Health widget

- ✔ A green check mark indicates that a best practice is being followed.

- ⚠ A yellow warning icon indicates that your configuration is not optimal.

- 🔔 A red icon indicates an error in your configuration.

  Fix all error conditions. You have the option to ignore warnings. They are provided to inform and encourage best practice configuration. You can accept warnings without fixing them.

- Select 📋 to accept the warning. If you accept a warning without fixing the configuration issue, a green warning icon displays ⚠.

- ⚠ A green warning icon indicates that you accepted the warning without fixing it.

- Select ❓ for a description of each statement or warning.

- Select ▤ to jump to that area in Extreme Campus Controller to improve your configuration.

Table 6 describes the best practice information that the widget provides.

Table 6: System Health Widget Best Practices

Type	Field	Description
Configuration	Scheduled Configuration Backup	It is a best practice to schedule a configuration backup. Automatically back up the configuration to a separate media or host. You can restore your configuration from a backup file in the event of a system failure. See Configure a Backup Schedule on page 300.
Configuration	TKIP	TKIP encryption is considered to be a less secure means of communication. An industry best practice is to use a more secure option for network privacy. Disable the TKIP option within the WPA2 privacy settings. See Privacy Settings for WPAv2 with PSK on page 185. A green check mark indicates that TKIP encryption is not used. A yellow warning condition indicates that TKIP encryption is enabled on a WLAN.
Configuration	APs adopted but not assigned to a site	APs must be part of a device group and assigned to a site. See Sites Overview on page 16.
Configuration	AP has configuration overrides	Indicates that there are APs in your network with configured override settings. For a consistent configuration, a best practice is to configure the APs through the configuration Profile. Overrides are available for unique configuration. However, variances from the configuration Profile can result in APs not receiving general policy changes. Consider configuration Overrides carefully. To determine which APs are configured with overrides, from the **AP List**, display the **Overrides** column. See Access Points List on page 50.
Configuration	WEP encryption for network privacy detected	The Wi-Fi Alliance™ recommends against using WEP encryption. WEP encryption is easily broken, often taking less than a minute to break. If you must use WEP, apply a restrictive policy to the associated VLAN to reduce your exposure after a breach.
Configuration	Open networks detected.	Networks with Open access pose a security risk for your organization. Consider an authentication type such as MBA or Captive Portal.
Configuration	Manufacturing Certificate	A Best Practice is to enforce enablement of Extreme PKI certificate in the establishment of secure tunnels.
Operational	Certificate Authentication	Pre-installed Extreme certificates allow validation between Extreme Campus Controller and an AP. APs that do not support signed certificates, can provide self-signed certificates. In this case, you must disable Enforce Manufacturing Certificate on Extreme Campus Controller for the AP. AP Authentication failure messages are logged in the Extreme Campus Controller Events Log.

Table 6: System Health Widget Best Practices (continued)

Type	Field	Description
Configuration	Multicast filters fully open	Multicast traffic can have a negative impact on performance. Ensure that multicast access is restricted per topology. See Configuring a Multicast Rule on page 227.
Configuration	Mesh Topology requires fixed channels	Mesh topology requires fixed channel assignment for proper access point operation. Do not use dynamic channel determination techniques such as ACS or Smart RF with a Mesh topology. Configure static channels through the AP Override settings. See Advanced Configuration and Mesh Point Profile Settings on page 98 and Advanced Setting Overrides on page 157.
Operational	Mesh does not use DFS channel	Due to DFS procedures and mandatory 'Stay off Channel' periods, APs operating on DFS channels in a Mesh topology can result in service outages.
Configuration	Mesh does not support Off-Channel Scan	**Note:** Supported on Extreme Campus Controller v5.16.03 with AP v7.5.1.2 or later. Mesh APs can be configured with fixed channels or RF Management Policy. When configuring fixed channels, configure both root and non-root APs on the same channel prior to deployment. For automatic channel selection, APs can use any RF Management Policy. Non-root APs will follow the channel and width of the root AP that it connects to. When using an RF Management Policy, non-root APs scan all channels on the selected band to find the root AP.
Configuration	Radio in sensor mode with no scan profiles assigned	Indicates that you have a radio in Sensor mode without a corresponding AirDefense or ExtremeLocation profile configuration. Scan functionality requires that you configure a radio for Sensor mode and configure Profile settings for AirDefense or ExtremeLocation. All configuration is handled in the configuration Profile that is assigned to the device group. See Add or Edit a Configuration Profile on page 95.
Configuration	Number of SSIDs per Radio	One radio can support a maximum of eight SSIDs. However, it is a best practice to configure no more than four SSIDs to a single radio. This configuration can be at the Profile level or configured as an override for a specific AP. See Add or Edit a Configuration Profile on page 95. A green check mark indicates that four or less SSIDs are configured. A yellow warning indicates that more than four SSID are configured for a single radio.

Table 6: System Health Widget Best Practices (continued)

Type	Field	Description
Configuration	Band steering enabled and 5GHz radio disabled	Client Band Steering steers dual-band capable clients to connect to the 5.0 GHz radio band instead of the 2.4 GHz radio band. A 5.0 GHz radio must be enabled on the AP for Client Band Steering to function. See Advanced Configuration Profile Settings on page 123.
Operational	AP recommended version image	APs are not running the recommended version image. Run the supported AP firmware version. Running other firmware revisions can lead to unexpected results. See Upgrade AP Images on page 304.
Configuration	40 MHz channel width on 2.4GHz radio	Operating a 40MHz channel in a 2.4 GHz band can cause co-channel inference with access points in the vicinity. The 2.4 GHz band has limited available channels. Therefore, for proper channel isolation, a 2.4 GHz band allows 3-4 (region dependent) 20 MHz channels. Best practice is to configure a 40MHz channel on a 5 GHz radio. See Channel and Power Settings on page 130.
Operational	AP with Dual 5 GHz and power provided is AF	AP510 and AP410 support Dual 5 GHz radios and AF (low power) is provided. Therefore, Radio 2 will be shut down. Configure the AP radio for 2.4 GHz or 5 GHz, or provide AT (high power).
Configuration	Smart RF monitoring disabled	Enable Smart RF for dynamic RF management to provide RF performance optimization. Enable Smart RF from the **Basic Settings** tab. See Basic RF Management Settings on page 128.
Configuration	Probe suppression threshold	Probe Suppression Threshold should not be greater than -70dB. The Probe Suppression Threshold defines the signal strength value that is deemed too low to be acknowledged by the AP. Setting the threshold above -70dB can result in an AP not acknowledging clients in close proximity, leading to poor connectivity or a sub-optimal roaming experience. The best practice is to follow the Site Survey methodology to determine the best value for the AP installation. See Advanced AP Radio Settings on page 106.
Operational	Backup secure tunnel	Secure tunnel is supported on ExtremeWireless Wi-Fi 6 APs. To improve resilience and reduce the outage interval associated with a failover event in a High-Availability pair, access points establish session tunnels to both peers in a High-Availability pair.
Configuration	Role with more than 64 rules is assigned to an AP or Profile that does not support more than 64 rules.	ExtremeWireless Wi-Fi 6 access points support rule sets that contain up to 256 rules. AP39xx series access points support rule sets with no more than 64 rules . See Add Policy Roles on page 214.

**Table 6: System Health Widget Best Practices (continued)**

Type	Field	Description
Configuration	Roles with more than 64 rules are configured.	Roles with more than 64 rules may experience interoperability issues with different AP models and firmware revisions.
Configuration	Network with CWA is assigned to non-supported APs	Support for Centralized Web Authentication (CWA) is only available on Wi-Fi 6 access points. This feature is not supported on AP3900 series access points. See Centralized Web Authentication on page 202.
Operational	NTP	Proper time stamp synchronization is facilitated through Network Time Protocol (NTP). If the NTP server is un-reachable, verify the NTP server settings. See Network Time on page 298.
Configuration	Device Registration is not configured on at least one port.	The Device Registration attribute controls whether access points and switches can establish management sessions with the controller through the selected interface. For proper system operation, at least one interface is required for managed devices to connect.
Operational	Service interface is not operational. Check connectivity for proper service.	System functions reference specific interfaces for connectivity. For proper operation, corresponding system interfaces must be enabled and operational.
Configuration	RADIUS Failover is not configured or there are not enough serves for redundancy	It is a best practice to configure at least one pair of RADIUS servers to support authentication redundancy.
Configuration	Bonded channels configured with a different frequency than the Management channel	Configure bonded channels with the same frequency as the Management channel. When channel width is larger than 20 MHz, use one 20 MHz sub-channel as a Management channel to transmit beacons. When Management channel frequency is configured differently than other channels, channel interference can occur and throughput is reduced.
Configuration	Default Route configured for router on data interface	Configure the Default Route/Gateway with a next-hop associated with a physical interface. Do not point the Default Route to the Admin interface. A best practice is to map the Default Route through a topology on a data port for proper system functionality. If necessary, configure the static routes via the Admin port for administration level access.
Operational	Backup tunnel established to Extreme Campus Controller	To improve resilience and reduce the outage interval associated with a failover event in a High-Availability setup. Access points establish session tunnels to both peers in a High-Availability Pair.
Operational	AP acknowledgment message	APs send an acknowledgment message for each configuration update. A missing configuration acknowledgment message from an AP can indicate a connectivity issue.

Table 6: System Health Widget Best Practices (continued)

Type	Field	Description
Operational	Communication between AP and controller over port 13910 is blocked by the firewall	For proper communication between the AP and the controller, ensure that Port 13910 is open in the firewall. **Note:** When the AP is more than one hop away, setting the default route via the Management port can also block communication between an AP and the controller.
Operational	AP connection to primary controller	In the event of an unexpected release of APs, check your network connectivity between APs and the controllers for possible interruptions.
Operational	Adoption rules did not successfully assign APs to site	Consider the following when configuring adoption rules for AP site assignment: • The selected AP Profile must match the AP hardware type. • The regulatory domain of the AP must match the Country setting for the site. For more information, see Adding or Editing Adoption Rules on page 234.
Operational	High Availability Configuration	High Availability connectivity status. Verify your High Availability configuration. See Availability on page 307.
Operational	High Availability Synchronization	High Availability connectivity status with synchronization message.

The notification icon indicates System Health warnings.

1. Select ![icon] at the top of your screen, then select **System Health**.
2. Select the three dots to display the warning messages.
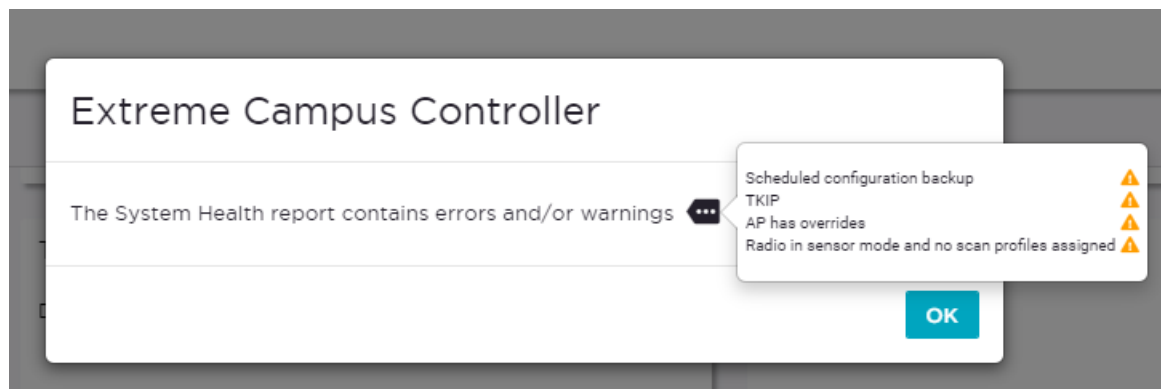
Figure 8: System Health Notification Report

Related Topics

Modify a Dashboard on page 29

Monitor

Sites List

Go to **Monitor** > **Sites** to view a list of sites configured in Extreme Campus Controller. 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 7: 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 150 • Radio Settings Button on page 39
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 Power level. • APs per Channel • Mitigation • Mitigation History

3. You can also:

   Select ✿ to modify configuration settings.

   Select ☰ to go back to the list.

Related Topics

Radio Settings Button

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

Table 8: Radio Settings

Field	Description
Set Tx Power	
Channel Width	Determines the channel width used by the channel on the selected radio. The channel width is set for all APs in a device group. Available options include: • 20 MHz • 40 MHz • 80 MHz (supported on 5GHz only 802.11ac and 802.11ax) • 160 MHz (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

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 9: Device Status from the Floor Plans View

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

Table 9: 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 140.
	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 115.

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.
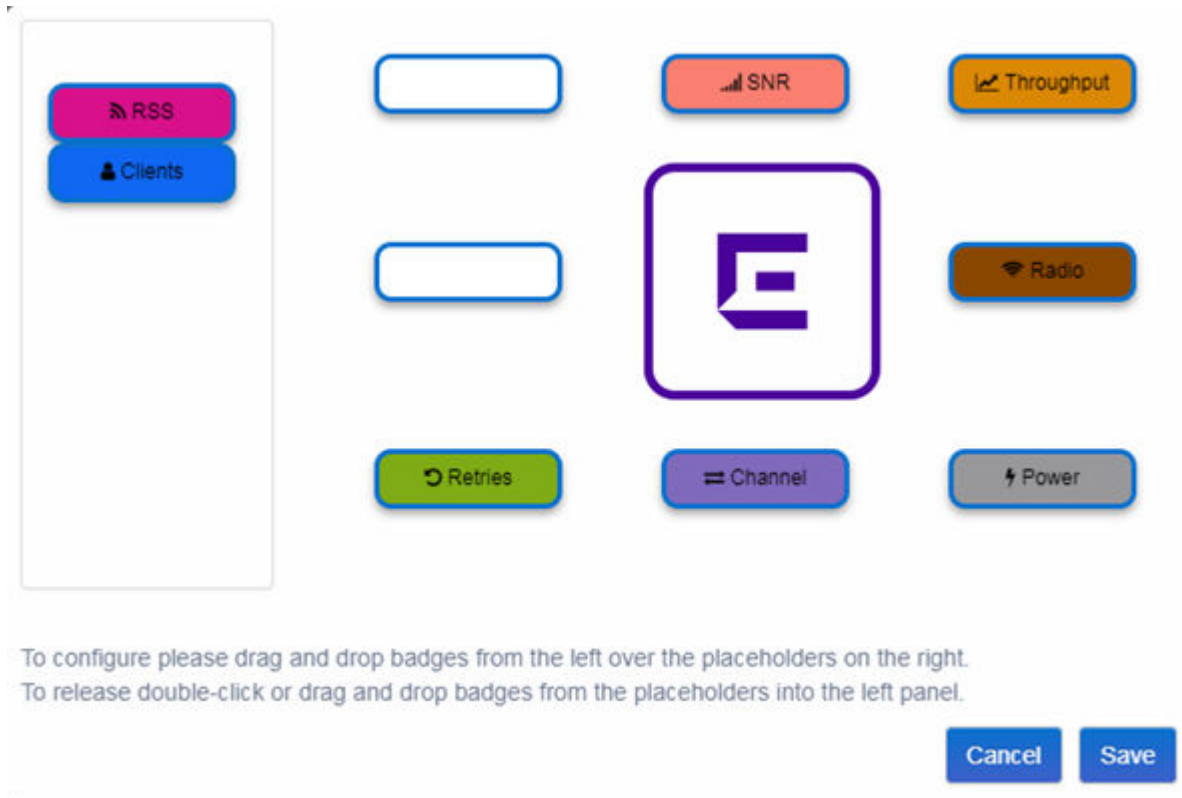
Figure 9: Badge Configuration Dialog

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.
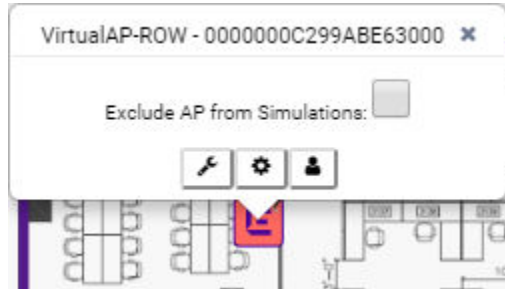
Figure 10: Device Context Menu

Related Topics

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 ☰.
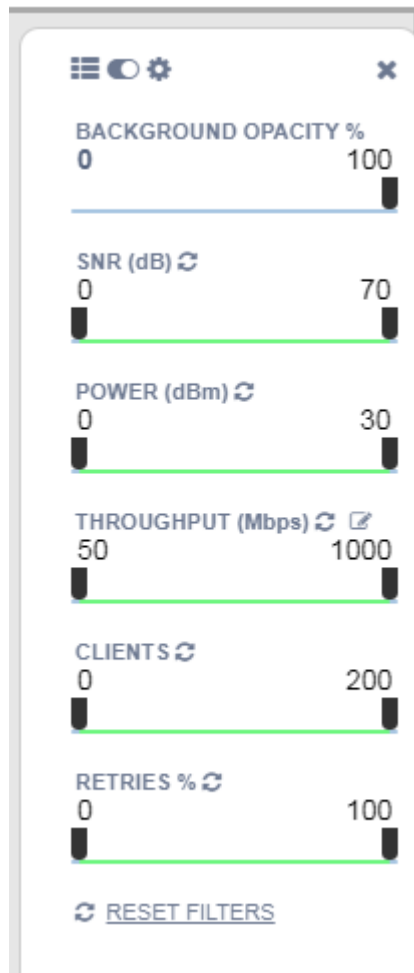
Figure 11: Map Filters Panel

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.
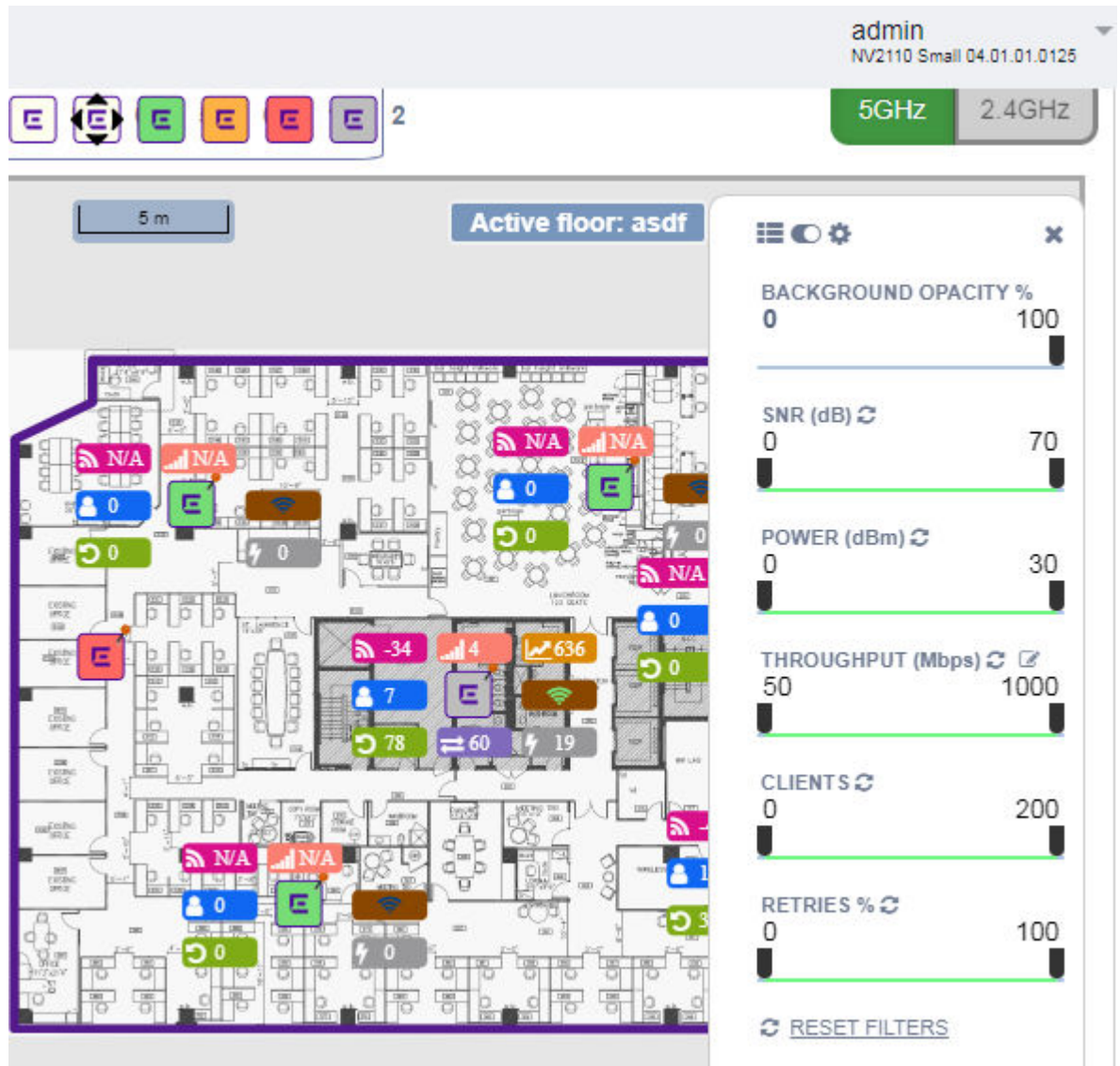
Figure 12: Badges that meet filter criteria appear on map

Understanding Readiness Maps

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

- Heat map. RSS signal strength.
- Heat map: BLE. Indicates expected coverage of Bluetooth Low Energy. Supported on the 2.4 GHz band for APs with a BLE radio.
- Channels map. Indicates AP channel with the strongest RSS.
- Link Speed.
- RFQI (RF Quality Index) of the radios 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.
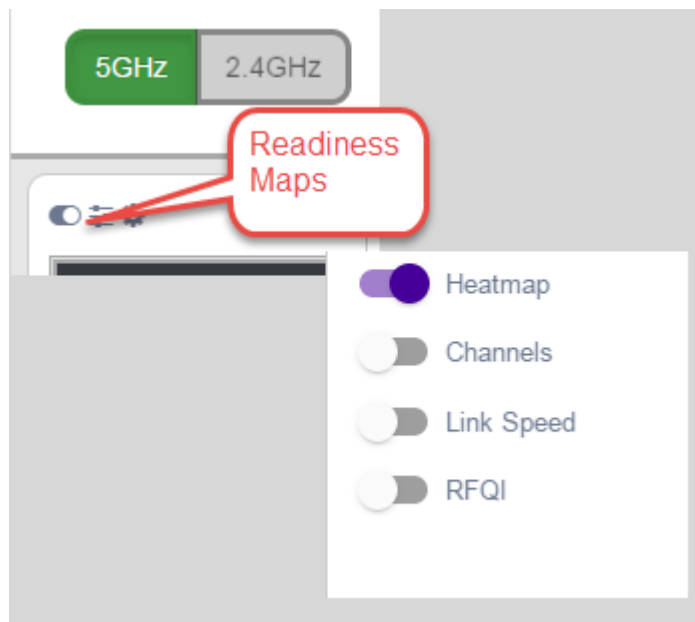
Figure 13: Network Readiness Maps

Right-click anywhere on a heatmap to view the numeric value at that location on the map.
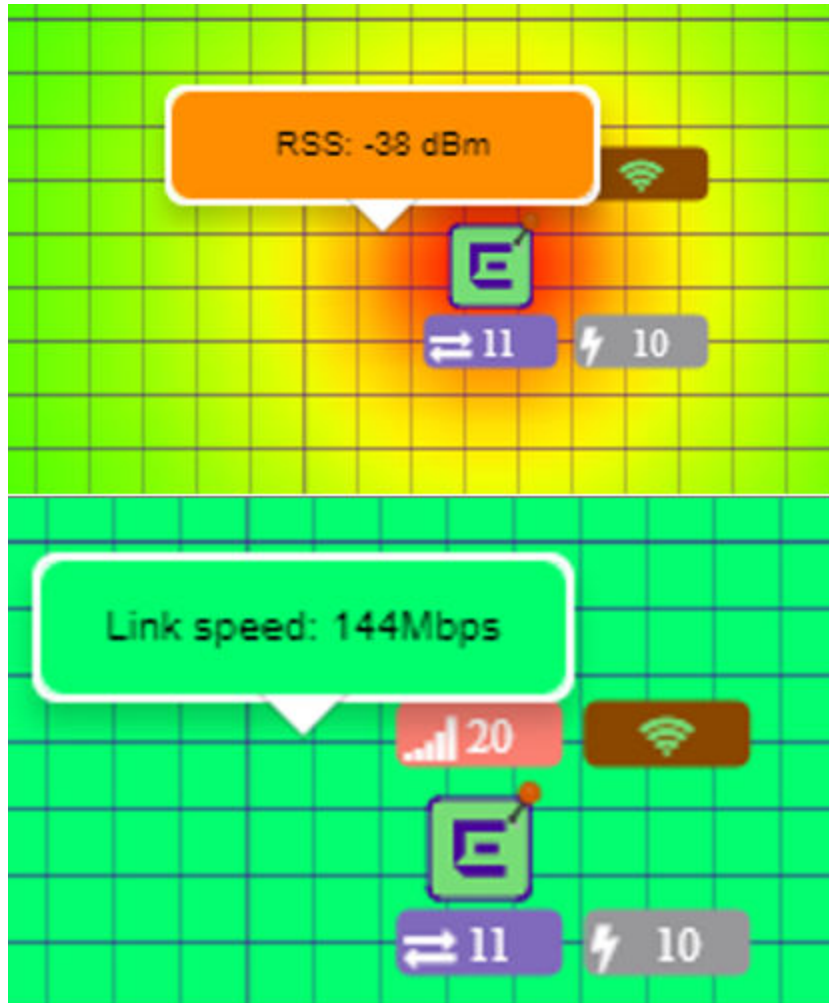
Figure 14: Push-Pin Reading for Heatmap Values

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

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

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

To access the Positioning maps from the floor plan view:

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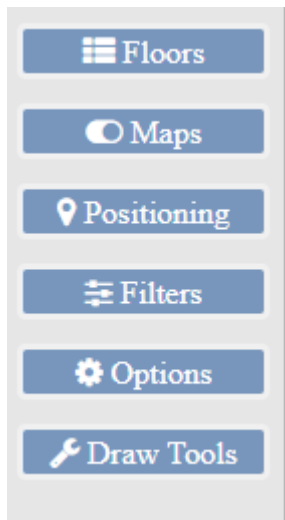
3. To activate a map, click the ball and drag to the right.
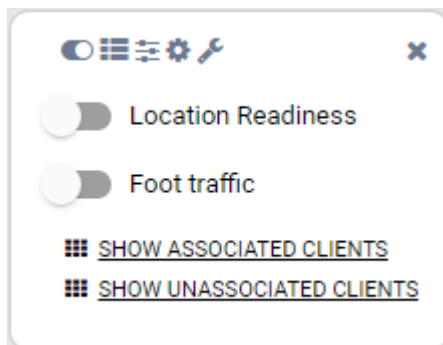
4. To show clients, select either **Show Associated Clients** or **Show Unassociated Clients**.

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

Related Topics

Device List

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

- See Access Points List on page 50 for a list of supported APs.
- See the Extreme Campus Controller Release Notes for a list of supported switches.
- Extreme Campus Controller supports Extreme Defender Adapter SA201 for the Defender for IoT solution. For more information on Extreme Defender for IoT, refer to documentation located in the Extreme Networks documentation portal.

Related Topics

Access Points List

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

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

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

Highlights on the **Access Points List**:

- The **MAC Address** column displays the AP MAC Address of the primary port. Use this information to identify the AP and facilitate integration processes.
- The **Profile** column indicates which configuration Profile the AP is associated with. A configuration Profile is defined at the device group. It applies configuration settings to the group.
- The **Radio 1 Clients** 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 105.
- The **Radio Mode** columns indicate the mode for each radio on the AP.

  Use the Radio Mode columns to indicate that an AP is configured as a Client Bridge. The Radio Mode column value for a Client Bridge AP is **bridge**.
- The **Adoption** column indicates if the AP is associated with the Primary or Backup Extreme Campus Controller in an availability pair. Use this information to understand an access point's home session. This value *does not* indicate where an AP may be currently connected in an availability pair.

- The **Overrides** column indicates that the AP has overrides. To view which override settings are enabled, select the AP and go to **Advanced** > **Overrides**.
- The **Ethernet Port Speed** and **Ethernet Port Mode** are available for a selected device.
- The **CERT** column indicates that a Certificate Signing Request (CSR) certificate has been applied to the AP.

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™ APs are supported:

- AP310i/e
- AP360i/e
- AP410i/e
- AP460i/e
- AP505i
- AP510i/e
- AP560i/h

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

The Extreme Networks Defender Adapter SA201 is supported.

For documentation on each AP model type:

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

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

Related Topics

Understanding Access Point States

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

Table 10: AP State from the Device List

State	Description
🟢	In-Service. Device has discovered Extreme Campus Controller and is providing service.
✳	Indicates which AP in a Distributed site acts as the domain manager (RFDM). The RFDM communicates directly with Extreme Campus Controller collecting statistics, access point upgrade information, and Smart-RF activities. Understanding which AP is the RFDM can help with troubleshooting.
⚠	In-Service Trouble. Device has discovered Extreme Campus Controller but it is not a member of a device group.
⚪	Unknown. Device is added to Extreme Campus Controller but the device has never discovered Extreme Campus Controller.
🟥	Critical. After being Active, Discovered, and On-boarded, associated device is no longer connected to Extreme Campus Controller.
🔵	Indicates that the AP is in the process of upgrading.

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

Query Builder

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

Build customized queries to filter data from the following areas in Extreme Campus Controller:

- **Monitor** > **Devices** > **Access Points** > **AP List**
- **Monitor** > **Clients** > **Client List**

- **Tools** > **Logs**.

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

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

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

Related Topics

Build a Query for Devices or Clients

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

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

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

   Go to **Configure** > **Devices** > **Access Points**.
2. To access the **Clients List** page, go to **Monitor** > **Clients**.
3. To open Query Builder, select ▼.
4. Select **Group**.

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

   - AND
   - OR

   > **Note**
   > AND is the only supported condition within a group.

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

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

   - Equals
   - Not Equals
   - Contains
   - Greater Than
   - Less Than
   - Less or Equals
   - Greater or Equals

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 **+**.

9. **Group** — Each group has conditions joined by the selected operator. You can add additional groups or add conditions to the group.

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

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

    > **Note**
    > Query Builder generates a Pandas query syntax. The syntax preview is displayed at the top of the **Query Builder** dialog. For saved queries:
    >
    > - Select 👁 to view the Pandas query.
    > - Select 📋 to copy the Pandas query to the clipboard.

Figure 15: Query Builder: Channel distribution by AP model per site

Select from the list of saved queries or create a new query.
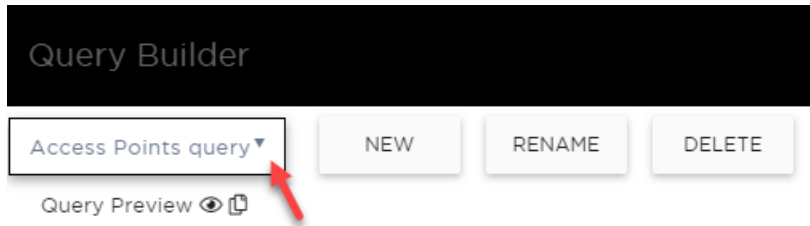
Figure 16: List of saved queries

Query Builder actions:

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

Related Topics

Visualize a Query

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

To visualize your query:

1. Select 🜨.
2. Select the column with the data element you want displayed.
3. Select **Render**.
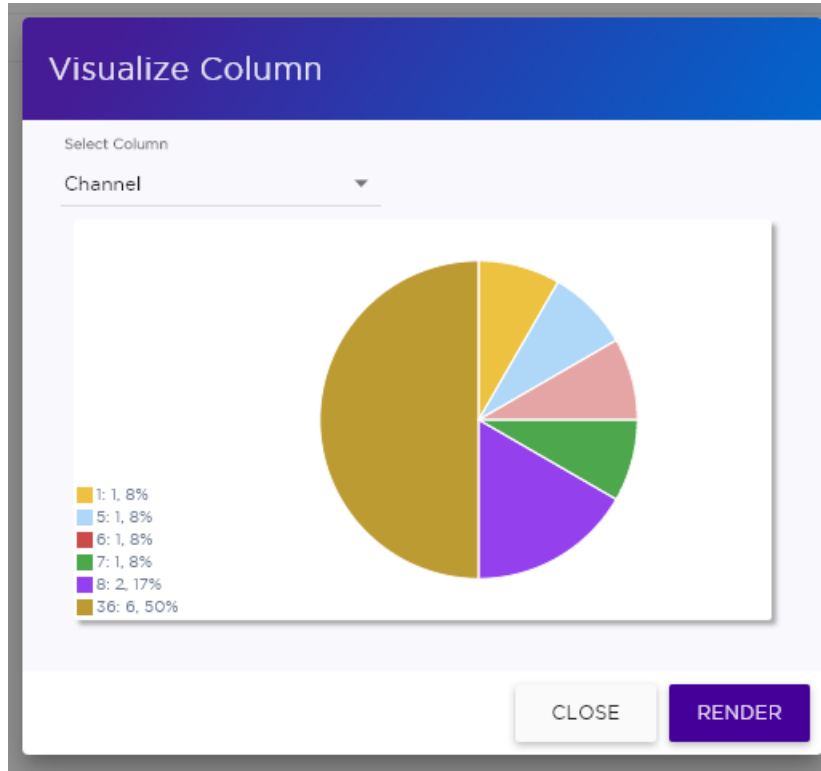
Figure 17: Channel Assignment for AP410i-CAN associated with Site Thornhill

The pie chart in Figure 17 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.
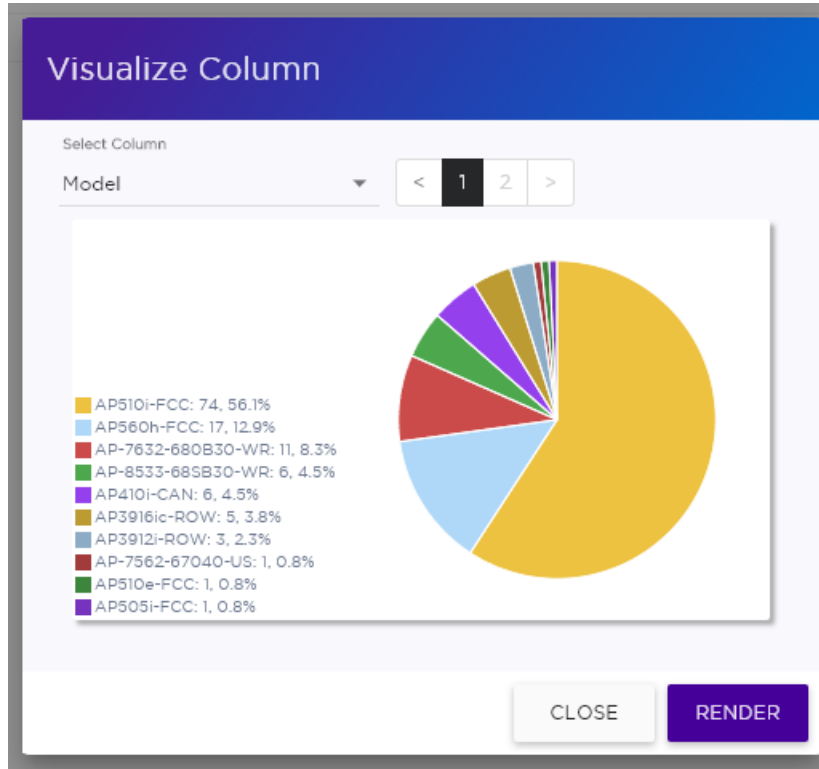
Figure 18: AP count by model number

Related Topics

Build a Query for Devices or Clients on page 53
Query Builder on page 52

Support for ExtremeWireless AP3xx Access Points

Extreme Campus Controller supports the ExtremeWireless™ AP310i/e indoor access point and the AP360i/e outdoor access point. These access points support users and internet of things (IoT) devices. In addition to both internal and external antennas, these APs support a Bluetooth Low Energy (BLE) antenna.

> **Note**
> AP3xx access points support is limited to Centralized sites.

- AP3xx, one dual band 2.4GHz/5GHz radio and one 5GHz radio.
  - Mode 1 — 2.4GHz service radio and 5GHz service radio
  - Mode 2 — 2.4/5GHz dual-band Sensor and 5GHz service radio
  - Mode 3 — 5GHz lower band service radio and 5GHz upper band service radio

  - Radio Channels:
    - Radio 1 can operate as:
      - 2.4GHz with all 2.4GHz channels
      - 5GHz with 5GHz lower band channels (channels 36-64)
      - 2.4/5GHz dual-band Sensor scanning on all 2.4GHz and 5GHz channels

- Radio 2 can operate as
  - 5GHz with 5GHz upper band channels (channels above 100)
  - 5GHz with 5GHz full channel list

Related Topics

Understand Radio Mode on page 104

Radio as a Sensor on page 105

Professional Install Settings on page 164

Support for ExtremeWireless AP4xx Access Points

Extreme Campus Controller supports ExtremeWireless™ AP410i/e and AP460i/e access points. The access points feature built-in dual-band radios, two band-locked radios, eight Wi-Fi 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.

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 104

Radio as a Sensor on page 105

Professional Install Settings on page 164

Support for ExtremeWireless AP5xx Access Points

Extreme Campus Controller 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.

- 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 11 and Table 12 on page 60 for descriptions of each product bundle.

Table 11: 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 12: 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 12: 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 104

Radio as a Sensor on page 105

Professional Install Settings on page 164

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 13: Tabs on the AP Details Screen

Tab	Description
Dashboard	Network charts provide client count and radio channel data. Use this information to determine network traffic associated with the AP and channel statistics.
Sites	Sites that include this AP. Click the site to show details.
Networks	List of network services associated with the device. Click a network to show network details.
VLANs	Details about AP Tunnel status for the selected AP and VXLAN information related to MTU packet size. For more information, see AP Tunnel Information on page 62. **Note:** Supported on AP3xx, AP4xx, and AP5xx models.
Roles	List of Roles associated with the device group, of which this device is a member.
Clients	List of clients associated with the AP. Add or remove clients from black and white lists.
Troubleshooting	Offers packet capture at the AP and remote console access to the AP.

Table 13: Tabs on the AP Details Screen (continued)

Tab	Description
Smart RF	View widgets that show information about the following: • Mitigation • Occupancy and neighbor channels • Peer AP visibility.
Certificate	Current credentials in use by the AP.

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, signal to noise ratio (SNR) levels, and client retry statistics.
- Clients. Provides metrics on client distribution by protocol, operating system, and manufacturer per AP.
- Expert: AP metrics for the expert user related to RFQI, RTT, RSS, and RX and TX Rates.
- Application Visibility. Provides details about applications the client is accessing and metrics on application groups related to throughput and usage per AP.

To view widgets for an individual AP:

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

Related Topics

NEW! *AP Tunnel Information*

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

> **Note**
> Supported on AP3xx, AP4xx, and AP5xx models.

To view tunnel status information:

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

AP Tunnel

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

IP Address

The IP address of the appliance. In an Availability Pair, the primary appliance is listed first.

Status

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

Configured MTU

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

Configured MTU Tunnel Status

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

Path MTU Learned by AP

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

Internal Management Tunnel

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

VLANS

The following information displays for a VxLAN topology:

Name

Topology Name

Mode

Topology type. Valid values are:

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

Tagged

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

VLAN ID

Identifies the VLAN.

I-SID

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

Certificates

Indicates that a certificate has been applied to the AP.

Remote VTEP

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

VNI

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

Tunnel Status

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

Related Topics

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 Extreme Campus Controller that is associated with the AP or site. To view the PCAP file, export the file to a host running Wireshark.

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

Extreme Campus Controller 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 Extreme Campus Controller in an Availability Pair. If the availability connection is disrupted, packet capture stops.

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

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.

- ExtremeWireless AP39xx and (AP3xx, AP4xx, and AP5xx) models:
  - Up to 4 IP filters can be applied
  - Up to 2 MAC filters can be applied
  - Capture wired and wireless packets simultaneously or independently
  - Capture packet refresh is supported
  - Live Packet Capture is supported.

Related Topics

Configure AP Packet Capture

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

Field Name	Field Description
In the **Capture Locations** pane, configure the following settings:	
Appliance Data Ports	Select this option to capture packets to and from the appliance. When capturing appliance data ports, you must configure at least one filter. From the **Add Filters** field, select either IP address or MAC address for the appliance. Only one capture task can apply to the Appliance Data Ports at a time. If more than one capture task is started using the Appliance Data Ports, the last requested task will be started.
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 3** — Enable packet capture on the AP4xx radio 3 (Sensor) interface. Available for AP4xx models only. You must configure an ADSP, Positioning, or ExtremeLocation profile to capture packets on the sensor radio. • **All Radios** — Enable packet capture on all radio interfaces for the selected AP. This option is selected by default. Note: AP39xx and AP3xx, AP4xx, 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.

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

Related Topics

Opening Live SSH Console to a Selected AP

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

To open a remote console to an AP:

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**.

Smart RF Widgets

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

> **Note**
> The Smart RF tools reflect data available for channels that are selected in the Channel Plan. For more information, see Channel and Power Settings on page 130.

- **Mitigation**. Mitigation action taken by Smart RF to improve the network:
  - Channel Change — The channel of an AP radio was changed
  - Power Change — The power of an AP radio was changed
  - Select Shutdown — AP radio shutdown
  - Coverage Hole — AP reacts to holes in AP coverage
- **Channel Energy**. Displays the amount of interference detected by each radio on each channel and indicates the source of the interference:
  - Neighbor Wi-Fi for APs
  - External Wi-Fi for non-neighbor sources of Wi-Fi interference
  - Non Wi-Fi Energy for interference that is not generated by a Wi-Fi signal
- **Channel Inspector**. Provides a high level of visibility as to the occupancy of the RF spectrum around a particular AP. The following data is provided on the widget:
  - Frequency. Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
  - Noise. Channel noise measured in Decibel-milliwatts (dBm).
  - Ranking. Indicates the best operating channel based on a 5-star ranking. This ranking is relative to the channels that are available. The higher the rank the more desirable the channel. The ranking algorithm considers the following parameters:
    - noise level
    - overlap count
    - co-channel count
    - adjacent AP count
  - Overlap. Number of APs on overlapping channels. Applicable for 40MGz and 80MGz channels only. The 20MGz channel is designated as the primary and the other channels are designated as extension channels (secondary). If the primary channel of one AP is the same as the extension channel of another AP it is considered overlapping. Overlapping is the worst type of interference.
  - Co-Channel. Number of co-channel APs. APs on the same channel as the target AP are competing. Using Distributed Control Function (DCF) collisions are avoided because the APs know to avoid each other; however, the more traffic on the channel the greater the chance of collisions. Throughput slows but all packets get through.
  - Adjacent. Number of APs on adjacent channels. Adjacent APs are close enough to interfere, but not close enough to know they are interfering. They do not have the benefit of DCF.

  To display more details for a specific channel, select a row in the widget. The Channel Inspector Interference Report displays.
- **Neighbor List**. Indicates channel occupancy and neighboring channels.

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

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

Figure 19 illustrates the following RF data for the selected site:

- Number of device groups with Smart RF Monitoring enabled.
- Number of device groups with Smart RF Monitoring disabled.
- Number of device groups using Automatic Channel Selection (ACS). AP39xx access points support ACS as the RF Management policy.
- Number of device groups using Static RF. Static RF represents APs not capable of Smart RF or ACS.
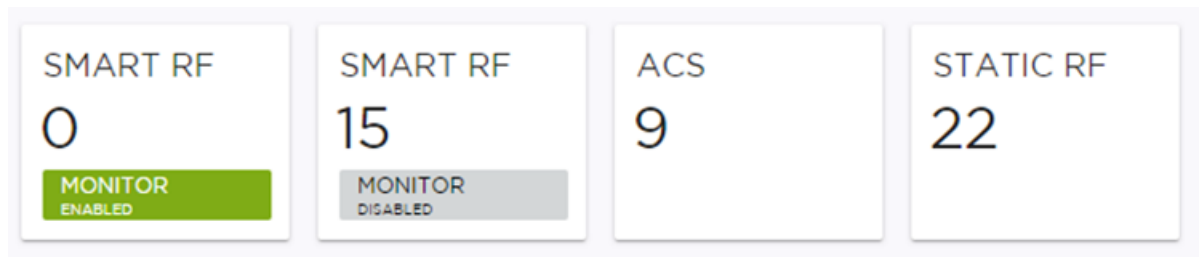
Figure 19: Smart RF data per site

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

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

Related Topics

        Channel and Power Settings on page 130

        Channel Inspector Interference Report on page 70

        Configuring RF Management on page 128

        Network Snapshot: Sites on page 38

Channel Inspector Interference Report

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

To access the Channel Inspector Interference Report, select a row on the **Channel Inspector** widget from the **AP Smart RF** dashboard.

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

> **Note**
> Smart RF data is available only when Smart RF is enabled and only for channels that are in the Smart RF channel plan. For more information, see:
> - Basic RF Management Settings on page 128
> - Scan Settings for Smart RF on page 134
> - Channel and Power Settings on page 130

Table 14: Channel Inspector Interference Report

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

Related Topics

Smart RF Widgets on page 69

Basic RF Management Settings on page 128

Scan Settings for Smart RF on page 134

Channel and Power Settings on page 130

Switches List

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

- To see a list of configured switches in Extreme Campus Controller , go to **Monitor** > **Devices** > **Switches**.

- To view a list of switches associated with a site, go to **Monitor** > **Sites**, select a site. Then, select the **Switches** tab.

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

Select ⟳ to refresh the data on demand.

Related Topics

Understanding Switch States

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

Table 15: 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 Extreme Campus Controller • Configuration is pending acknowledgment from switch • Switch reset pending • Switch reboot pending • Switch upgrade pending
⚫	Unknown. Switch has not discovered the Extreme Campus Controller.
🟥	Critical: • Switch stops sending requests for 5 minutes or longer • Consistent with a lost of connectivity to Extreme Campus Controller

Network Snapshot: Switch Details

To view network details from the switch screen:

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

   The network details for the selected switch display.

Table 16: Tabs on the Switch Details Screen

Tab	Description
Dashboard	Widgets display network details related to the selected switch.
Ports	A list of configured ports on the selected switch.
LAG Ports	Link Aggregation Group (LAG) Ports organized as a list of master ports and the LAG members that are associated with the master port. All ports assigned to a LAG must have the same port function. The configuration of the master port is shared with its LAG members. When a port is added to a LAG, its previous unique configuration is removed and the port inherits the group configuration. **Note:** A Link Aggregation Group whose function is to connect to an AP is limited to two ports in the group. Both ports must negotiate to the same speed (1 Gbps). LAG is supported on ExtremeWireless AP39xx and 11ax APs in a Centralized site.
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 74

Ports List on page 74

LAG Ports on page 75

Traces on page 75

VLANS on page 76

Troubleshoot a Switch Using the CLI on page 75

Configure a Switch on page 173

Switch Port Configuration on page 174

Port Dashboard on page 74

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 74
Switch Port Configuration on page 174

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 174

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 174

Traces

Trace information related to the selected switch.

Troubleshoot a Switch Using the CLI

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

> **Note**
> Extreme Campus Controller remote console to a switch *does not* support 200 Series switches.

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

To access the live console from the switch **Troubleshooting** tab, the ExtremeXOS switch must be in GUI-Mode. To set the switch mode, select the settings button ⚙ and then select **Advanced**. For more information on Switch mode, see Access the Switch CLI on page 177.

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 Extreme Campus Controller credentials.
4. To terminate the console session, select **Disconnect**.

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

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

For information on ExtremeXOS CLI commands, see ExtremeXOS documentation.

Related Topics

Access the Switch CLI on page 177

Advanced Switch Settings on page 176

Switch Configuration Backup Files on page 178

VLANS

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

Related Topics

VLANS on page 223

Networks List

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

Related Topics

Network Snapshot: Network Dashboard on page 76

Network Widgets on page 77

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 17: 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 77

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.
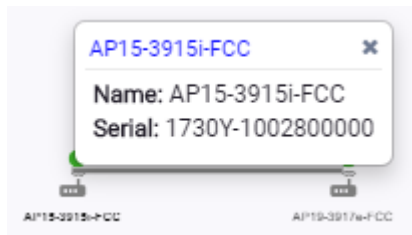
Figure 20: Mesh Node Details

- To display **Link Information**, select the line connecting the nodes. This shows link information from the child AP perspective only.
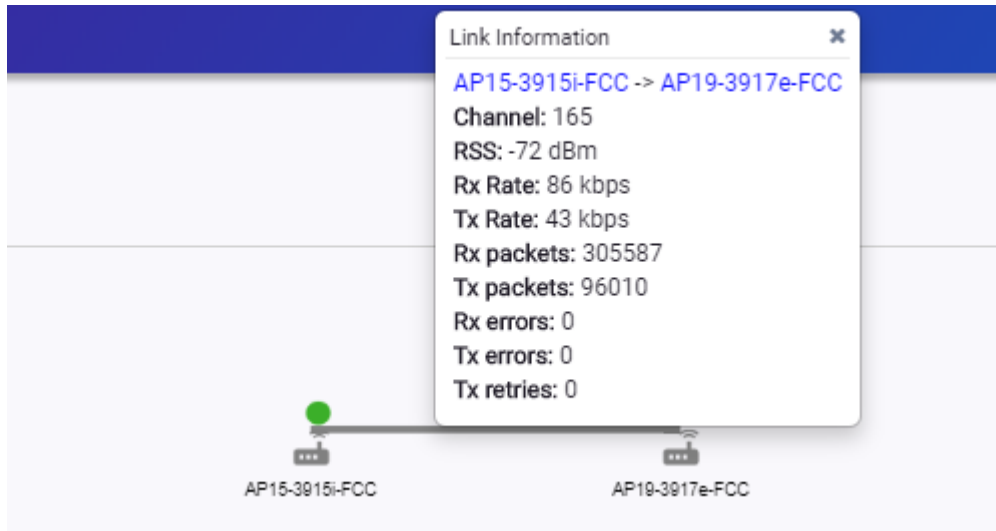
Figure 21: Mesh Link Information

- ◦ Channel
- ◦ RSS dBm
- ◦ 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 22: Navigation Buttons

- Zoom in and out using the zoom buttons.

Figure 23: Zoom Buttons

- To center the diagram, select ⊗.

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

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.

Highlights on the **Clients List**:

- IP Address — The IP Address field displays the IPv4 address and indicates when there is up to three IPv6 addresses. Hover over the IP Address field to view the full IPv6 address. You also have the option to display the IPv6 addresses in a separate field.
- RSS (dBm) — Received Signal Strength Indicator is the estimated power level that a client device is receiving from the associated access point.
- Spatial Stream — Number of MIMO streams supported by each client. Use this information to inform your decisions about hardware purchases and decisions about network configuration.
- Capabilities — Client protocol capabilities. Indicates which protocol capabilities the client supports. Valid values are:
  - PMF (Protected Management Frame) — PIM (Protocol Independent Multicast) Flooding Mechanism.
  - RRM — Radio Resource Management
  - WPAv1/WPAv2/WPAv3 — Wi-Fi Protected Access (versions 1-3)
- DL Lost Retries Packets — Indicates the number of packets lost between the AP and the client (downlink). This value indicates the health of the RF environment. Possible reasons for packet transmission failure are channel noise or co-channel interference.
- DL Lost Retries Bytes — Indicates the number of bytes lost in packet transmission between the AP and its clients (downlink). This value indicates the health of the RF environment. Possible reasons for packet transmission failure are channel noise or co-channel interference.
- Channel — Indicates the channel to which the client is connected. Possible values include a specific channel number or a channel number, plus offset, and channel width.

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

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

Select a client to see client details.

Related Topics

Understanding 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 $\circlearrowright$ 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 Extreme Campus Controller or by an Extreme Campus Controller 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

Managing Access Control Rules on page 274

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.

Delete

Disassociate

Reauthenticate

Add to Group

Remove from Group
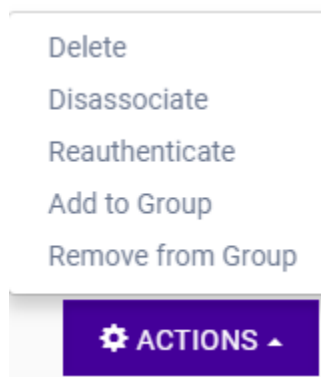
⚙ ACTIONS ▲

Figure 24: Client Actions Button

Table 18: 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 Extreme Campus Controller before the wireless service is restored.

Table 18: Client Actions (continued)

Field	Description
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 19: 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 20: 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 180 .
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 85

Station Events on page 83

Client Actions on page 81

Understanding Date and Time on page 25

Overview Dashboard on page 26

Floor Plans on page 20

System Logging Configuration on page 319

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 21 are documented in alphabetical order.

Table 21: 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.

Table 21: End-System Event Fields (continued)

Field	Description
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.
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

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

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

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.

Extreme Campus Controller is shipped with a default policy configuration that includes the following default roles:

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

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

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

Related Topics

Add Policy Roles on page 214
Role Widgets on page 87
Policy Role Settings on page 214

Preconfigured Policy Roles

Extreme Campus Controller is shipped a with the following default policy configurations listed in Table 22.

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

Table 22: Preconfigured Policy Roles

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

Table 22: Preconfigured Policy Roles (continued)

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

Related Topics

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

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

Figure 25: 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 26: Top Rules by Hit Count on the Roles Dashboard

Figure 27: 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 Extreme Campus Controller reporting duration is supported. Live reporting is not supported.

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

> **Note**
> Hit Count reporting is synchronized within an Availability Pair.

Configure

Network Configuration Steps

The following is the basic workflow for setting up your network using Extreme Campus Controller:

> **Note**
> To ensure the devices discover Extreme Campus Controller, configure DHCP, NPS, and DNS Services for Extreme Campus Controller discovery. For more information, see the *Extreme Campus Controller Deployment Guide* located in the Extreme Networks documentation portal.

> **Note**
> Users with Read-Only access to Extreme Campus Controller do not have access to the Extreme Campus Controller configuration options.

1. Create one or more sites.

   Select a Country for the site. The Country option affects the licensing domain associated with the site.

2. Configure one or more device groups for each site.

   A device group is defined by the AP platform. It contains APs with the same model type. The configuration Profile and RF Management profiles are defined at the device group level. The available configuration options depend on the AP platform definition of the device group.

3. Configure one or more networks. When configuring a network, you will do the following:

   a. Define network authentication.

   b. Configure roles associated with the network.

   c. Configure VLANs associated with the network.

4. Configure Adoption Rules so that new APs are automatically assigned to the appropriate device group based on factors such as AP platform, IP address, host name, or serial number.

5. (Optional) Configure additional roles.

6. Go back to each device group and associate the configured networks and the defined roles by editing the assigned configuration Profile. Alternatively, you can associate the Profile with the network or policy definition during the initial configuration of the network or role. For more information, see Associated Profiles on page 98.

7. Install and add devices.

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

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

   - If you have a device group with a valid profile and a valid adoption rule, the APs are automatically added to the proper device group.
   - If you have a device group with a valid profile, but no adoption rules, the APs are listed in the device group where you can manually add them to the group.
   - If you do not have a valid device group for the AP, the AP is listed on the **Devices** list with an *In-Service Trouble* status. 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

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

Related Topics

Add a Site

To add a site to Extreme Campus Controller, 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 23: Site Configuration Parameters

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

Related Topics

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

RADIUS Configuration for Switches Per Site

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

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

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

1. Configure each RADIUS server.

    Go to **Onboard** > **AAA** > **RADIUS Servers**.

2. Associate the RADIUS servers to the switches within the site configuration.

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

    MSTP

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

    AAA Policy

    Refer to external RADIUS servers directly without proxy by NAC. For configuration steps, see Configure AAA Policy on page 243.

    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. Your site location is automatically displayed based on data in the geodatabase served from your browser. You can also select a location on the map to populate the Map Coordinates field, or type specific coordinates in this field.

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

4. Select **Save**.

Related Topics

Site Parameters on page 92

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 17.

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 Groups on page 17

Device Group Parameters on page 95

Profiles on page 18

RF Management on page 19

Adoption Rules on page 234

Device Group Parameters

Configure the following parameters:

Table 24: 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. Extreme Campus Controller includes a default RF policy. • AP 39xx access points support Default ACS. • AP3xx, AP4xx, and AP5xx access points support 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

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

New Profiles display the configuration settings that were delivered with your initial Extreme Campus Controller installation. After making changes, if you need to return to a base Extreme Campus Controller configuration, create a new Profile for the AP platform. The new Profile will consist of the initial settings.

Before configuring a unique configuration Profile, configure the networks and roles associated with the new Profile.

1. Go to **Configure** > **Sites** and select a site.
2. Select the **Device Groups** tab.
3. To add a new device group, select **Add**. Or, select a device group from the list.
4. From the **Profile** field, select ⊕ to configure a new Profile or select ✎ to edit the Profile.
5. Configure the following parameters:

Table 25: 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.
Mesh Points	Define mesh points for a wireless mesh network. Extreme Campus Controller allows one mesh point per AP. For more information, see Advanced Configuration and Mesh Point Profile Settings on page 98.
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 86 • Add Policy Roles on page 214
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 104. • **Client Bridge Network** - Network associated with the Client Bridge. This field displays when Radio Mode is **Client Bridge**. For more information, see Configure Client Bridge on Extreme Campus Controller on page 101. For each radio band, select **Advanced** to configure Advanced AP Radio Settings.
Wired Ports	If the AP supports wired ports, configure port speed for each port. Valid values are: • Auto • 100M • 10M

Table 25: Profile Configuration Parameters (continued)

Field	Description
VLANS	Topologies associated with the configuration Profile. Associate a topology to a specific device group. This allows you to define a topology that is common to a set of devices and specify a specific attached VLAN. Topologies referenced by attached networks or roles are automatically added to the Profile VLANS list. You can also add topologies manually to the list. When creating a new topology, select the Profiles to associate with the new topology. For more information, see Configuring VLANS on page 224.
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 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, AP3xx, AP4xx, and AP5xx.
Analytics	Select a configured ExtremeAnalytics Profile. Or, Select 🔘 to add a new Profile. Select ✎ to edit the selected Profile. **Note:** Supported on AP39xx, AP3xx, AP4xx, and AP5xx.
RTLS	Select a configured RTLS Profile. Or, Select 🔘 to add a new Profile. Select ✎ to edit the selected Profile.

Related Topics

NEW!Associated Profiles

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

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

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

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

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

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

Related Topics

Profiles on page 18

Add or Edit a Configuration Profile on page 95

VLAN Profile Settings on page 112

Advanced Configuration and Mesh Point Profile Settings

The Mesh APs use wireless beacons to advertise their capabilities. Mesh APs connect to each other using the information in the beacons. One mesh point per AP is supported.

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

Both bridged WLAN services and tunneled WLAN services are supported.

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

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

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

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

- Configure only one AP radio for Mesh Point. Each AP is limited to one mesh point.

- Radio settings for the root-AP and non-root APs must match.

- When you add or remove a mesh point from a radio, the AP will reboot.

- Dual-band support is available with Mesh Point. When one radio is configured for Mesh Point, the second radio can provide service.

- Mesh APs can be configured with fixed channels or RF Management Policy. When configuring fixed channels, configure both root and non-root APs on the same channel prior to deployment. For automatic channel selection, APs can use any RF Management Policy. Non-root APs will follow the channel and width of the root AP that it connects to. When using an RF Management Policy, non-root APs scan all channels on the selected band to find the root AP.

> **Note**
> Supported on Extreme Campus Controller v5.16.03 with AP v7.5.1.2 or later.

- The recommended Poll Timeout setting for non-root APs is 60 seconds.

> **Note**
> Configuration parameters you set from the configuration Profile apply to all APs in a device group. To override settings for specific AP, go to the AP radio properties. For more information, see Advanced Setting Overrides on page 157.

To configure Mesh Point settings in a configuration Profile:

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:

Table 26: AP Mesh Point Settings

AP Model	Option	AP Behavior
• AP3xx • AP4xx • AP5xx	Root **Note:** Wi-Fi 6 access points: AP3xx, AP4xx, and AP5xx can be part of the same mesh network, but they cannot participate in a mesh network with AP39xx. AP39xx access points must be a separate mesh network from the Wi-Fi 6 APs.	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. Select the root behavior of this mesh point. • **Yes** - Mesh point is root node for this mesh network. • **No** - Mesh point is not a root node for this mesh network.
AP39xx	Root	• **Yes** - Mesh point is root node for this mesh network. • **No** - Mesh point is not a root node for this mesh network. **Note:** When using an AP39xx: • 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.
AP39xx Only	Path Selection Method	Select the method used for path selection in a mesh network. Available options include: • Uniform – The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths). Use this method for regular infrastructure meshing. • SNR-Leaf – Use this method in special infrastructure cases when it is more desirable to make path decisions based on SNR than on metric values.
AP39xx Only	Hysteresis Minimum Threshold	This is the minimum SNR value to consider a candidate for the next hop in a dynamic mesh network. For the AP39xx, this value maps to the Roaming Threshold value. • 100dB to 85dB maps to Low • 84dB to 70dB maps to Medium • 69dB to 0dB maps to High

Related Topics

Configure Client Bridge on Extreme Campus Controller

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

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

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

> **Note**
> Consider the following when configuring a radio as a Client Bridge:
>
> - Only one radio can be configured as a Client Bridge. This can be either radio. Regardless of which radio is configured as the Client Bridge, both radios will continue to provide service.
>   - Radio 1 enables Client Bridge on the 2.4GHz band only.
>   - Radio 2 enables Client Bridge on the 5GHz band only.
> - The Client Bridge radio will connect on the radio channel that is determined by the infrastructure AP.
> - Eight networks can be configured per radio. If one network is configured as a Client Bridge, seven additional networks can be configured for service on that radio.

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

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

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

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

Figure 28: Configuration Profile with Client Bridge Configuration

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

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

6. From the configuration Profile **Advanced** settings, the **GE2 Port Function** is automatically set to **Client** after configuring the Client Bridge radio.
7. Save the configuration Profile.
8. If you are planning to connect the end-system to the Client Bridge AP through the GE2 port, edit the configuration Profile again.

9. On the **Networks** tab, the Client Bridge network is indicated with a black highlight.

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

NETWORKS	MESHPOINTS	ROLES	RADIOS	WIRED PORTS	AIR DEFENSE	EXTREMELOCATION

Name	Radio 1 - 2.4GHz	Radio 2 - 5GHz	ge2
CB_Network	☑ *	☐	☑
DFNDR_Service	☐	☐	☐
test1	☑	☐	☐

* WLAN is used as primary BSSID. Removing WLAN will cause radio reset.

Figure 29: Configuration Profile Network Configuration – Client Bridge

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

    Only allow 1 network assign to Client Bridge and GE2 interfaces respectively.

11. Connect the Client Bridge AP to Extreme Campus Controller using the GE1 Port, which is designated as the primary port.

12. Assign Client Bridge AP to device group and assign the device group to the site.

13. After the Client Bridge link is established, disconnect the Client Bridge AP from the GE1 Port and Extreme Campus Controller.

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

The end-system device traffic is connected through GE2 port. The Client Bridge AP communicates with the infrastructure AP on the wireless network.

Related Topics

Understand Radio Mode

Extreme Campus Controller presents valid values for Radio Mode based on the AP capability.

> **Note**
> Sensor mode converts the radio to a sensor for ADSP, ExtremeLocation, and Positioning. The access point models AP4xx offer a separate sensor radio. For more information, see Radio as a Sensor on page 105.

Table 27: Radio Modes

AP Model	Radio 1	Radio 2	Radio 3 (Sensor)
AP310i/e	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • Client Bridge (2.4 GHz only)	5GHz • sensor • a/n/ac • a/n/ac/ax • Client Bridge (5GHz) **Note:** When selecting Client Bridge (5GHz) on Radio 2, Radio 1 forwards traffic on a 2.4 GHz band only.	
AP360i/e	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • Client Bridge (2.4 GHz only)	5GHz • sensor • a/n/ac • a/n/ac/ax • Client Bridge (5GHz) **Note:** When selecting Client Bridge (5GHz) on Radio 2, Radio 1 forwards traffic on a 2.4 GHz band only.	
AP410i/e	2.4GHz • b/g • g/n • b/g/n • g/n/ax • Client Bridge	5GHz • a/n/ac • a/n/ac/ax • Client Bridge (5GHz)	2.4GHz /5GHz (dual band) • sensor (non-configurable)
AP460e	2.4GHz • b/g • g/n • b/g/n • g/n/ax • Client Bridge	5GHz • a/n/ac • a/n/ac/ax • Client Bridge (5GHz)	2.4GHz /5GHz (dual band) • sensor (non-configurable)

Table 27: Radio Modes (continued)

AP Model	Radio 1	Radio 2	Radio 3 (Sensor)
AP505i	2.4GHz • sensor • b/g • g/n • b/g/n • g/n/ax • Client Bridge	5GHz • sensor • a/n/ac • a/n/ac/ax • Client Bridge (5GHz)	
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 • Client Bridge (2.4 GHz only)	5GHz • sensor • a/n/ac • a/n/ac/ax • Client Bridge (5GHz) **Note:** When selecting Client Bridge (5GHz) on Radio 2, Radio 1 forwards traffic on a 2.4 GHz band only.	
AP560i/h	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • Client Bridge (2.4 GHz only)	5GHz • sensor • a/n/ac • a/n/ac/ax • Client Bridge (5GHz) **Note:** When selecting Client Bridge (5GHz) on Radio 2, Radio 1 forwards traffic on a 2.4 GHz band only.	
AP39xx	5GHz • sensor • a/n/ac • ac-strict	2.4GHz • sensor • b/g • g/n • b/g/n • g/n-strict	

Related Topics

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 ExtremeWireless access points. On AP39xx, 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 AP3xx and AP5xx, the sensor can be set per radio — one radio can be configured as a sensor, and the other one can be configured to pass wireless traffic. The AP310 and AP510 are dual-band APs. A white LED indicates sensor selection. 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 123

Add or Edit a Configuration Profile on page 95

NEW!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 AP3xx, AP4xx, and AP5xx models. 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: • AP310i/e • AP360i/e • AP410i/e • AP460i/e • 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
Guard Interval Mode	The guard interval is the space between characters being transmitted (not the space between packets). The default value is **Auto**, which is sufficient for most indoor deployments. Consider **Long** or **Quadruple** for outdoor deployments where devices are installed more than 100 meters away. Setting the Guard Interval to Long or Quadruple, gives each AP more time to detect the received signal, improving signal quality, but sometimes reducing signal throughput. Valid values are: • Auto • Long • Short • Quadruple Quadruple is the longest setting. It is applicable in 802.11ax mode only. **Note:** Supported on AP3xx, AP4xx, and AP5xx models.
Airtime Fairness Mode	Enabling Airtime Fairness organizes radio traffic allocating bandwidth to faster devices. If you have older devices on your network that are hogging bandwidth, consider enabling Airtime Fairness to give priority to faster devices.
Maximum Distance	Increasing the Maximum Distance can give APs in an outdoor deployment more time to receive acknowledgment messages. For outdoor deployments, where APs are installed more than 100 meters apart, consider increasing the Maximum Distance setting up to 15000 meters.
Tx Beam Forming	Tx Beam Forming is a technique of re-aligning the transmitter multipath spatial streams phases in order to get better signal-to-noise ratio on the receiver side. Support is based on AP model number: • AP 39xx — Available on the 5GHz radio only. The valid values are: (multi-user) MU_MIMO and Disabled. • AP3xx, 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 6, 9, 12, 18, 24, 36, 48, and 54. The default value is 6.

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 Sub-frames	Maximum number of sub-frames of the MAC Protocol Data Unit (MPDU) aggregation.. The value range is 2-64.
DTIM	When any single wireless client associated with an access point has 802.11 power-save mode enabled, the access point buffers all multicast frames and sends them only after the next DTIM (Delivery Traffic Indication Message) beacon, which may be every one, two, or three beacons (referred to as the "DTIM interval").
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: • AP310i/e • AP360i/e • AP410i/e • AP460i/e • 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: • AP310i/e • AP360i/e • AP410i/e • AP460i/e • 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: • AP310i/e • AP360i/e • AP410i/e • AP460i/e • AP505i • AP510i/e • AP560i/h
Cell Size Control	
Probe Suppression on Low RSS	Reduces the number of probe responses by preventing clients with low RSS from associating with an AP radio. This setting is configured per radio. Clients with RSS measured below the Probe Suppression RSS Threshold will not associate with the AP. This setting is disabled by default.

Table 28: Advanced Radio Settings (continued)

Field	Description
Probe Suppression RSS Threshold (dBm)	This setting is available when **Probe Suppression on Low RSS** is enabled. This setting determines the RSS threshold for forced disassociation and probe suppression. The default threshold is -90 dBm. Valid value range is -50dBm to -100dBm. **Best Practice:** Probe Suppression Threshold should not be greater than -70dB. The Probe Suppression Threshold defines the signal strength value that is deemed too low to be acknowledged by the AP. Setting the threshold above -70dB can result in an AP not acknowledging clients in close proximity, leading to poor connectivity or a sub-optimal roaming experience. The best practice is to follow the Site Survey methodology to determine the best value for the AP installation.
Disassociate on Low RSS	This setting is supported on AP39xx, AP3xx, AP4xx, or AP5xx, (in a Centralized Site). It is always disabled by default. This setting forces clients with low RSS to disassociate from an AP radio. This setting is configured per radio. A client is forced off an AP radio when RSS is measured at 5dBm below the Probe Suppression RSS Threshold. Enabling this option forces a client to roam to a better AP for improved network performance.
Probe Response Retry Limit	The default Probe Response Retry Limit is 4. If devices are having a problem connecting to the network, due to congestion or due to the quality of the device, consider increasing the retry limit. Maximum value is 10.
Rx Sensitivity Reduction (dB)	New APs are very sensitive and can pick up unwanted channel interference. If this is an issue, add an offset of 5-10 dB, which will reduce signal sensitivity and improve signal quality.

Related Topics

NEW! VLAN Profile Settings

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

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

Related Topics

AirDefense Profile Settings

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

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

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

1. Configure the following settings:

Table 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 Extreme Campus Controller data port that is reachable by the APs and sensors.
Port	Specify a port for the AirDefense server. The default port is 443 (used with a dedicated external AirDefense Server). **Note:** When using the AirDefense Base (add-on container application), configure port number to **32032**.
Servers	List of IP addresses for servers. Click 🗑 to remove an IP address from the list.

2. Select **Save**.

Related Topics

ADSP Support on .11ax APs

The following ADSP features are supported on the AP3xx, 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 not* supported on ExtremeWireless AP39xx.

Related Topics

AirDefense Profile Settings on page 113

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 Extreme Campus Controller Positioning and ExtremeLocation at the same time. RSS information travels both through the WASSP tunnel to the Extreme Campus Controller 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 Extreme Campus Controller 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 Extreme Campus Controller, 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

Radio as a Sensor on page 105

Add or Edit a Configuration Profile on page 95

IoT Profile Settings

Extreme Campus Controller supports the IoT applications listed in Table 31.

Table 31: IoT Application Support

Application	AP Models Supported
iBeacon	• AP310i/e • AP360i/e • AP410i/e • AP460i/e • AP505i • AP510i/e • AP560i/h • AP391x **Note:** AP3935, AP3965 do not support IoT.
iBeacon Scan	• AP310i/e • AP360i/e • AP410i/e • AP460i/e • AP505i • AP510i/e • AP560i/h • AP39xx
Eddystone-url Beacon	• AP310i/e • AP360i/e • AP410i/e • AP460i/e • AP505i • AP510i/e • AP560i/h • AP39xx

Table 31: IoT Application Support (continued)

Application	AP Models Supported
Eddystone-url Scan	• AP310i/e • AP360i/e • AP410i/e • AP460i/e • AP505i • AP510i/e • AP560i/h • AP39xx
Thread Gateway	• AP310i/e • AP360i/e • AP410i/e • AP460i/e • AP505i • AP510i/e • AP560i/h • 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.

Table 32: iBeacon IoT Settings (continued)

Parameter	Description
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**. Extreme Campus Controller 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.
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.

Table 33: iBeacon Scan Settings (continued)

Field	Description
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. Extreme Campus Controller forwards data with matching UUID to the Application Server and filters out all other UUID data. If UUID configured value is all zeros, no filtering occurs.
Min RSSI	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.
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, AP5xx, and AP4xx.

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.

Table 36: Thread Gateway Settings (continued)

Parameters	Description
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 Extreme Campus Controller.

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, AP3xx, AP4xx, and AP5xx.

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

> Add or Edit a Configuration Profile on page 95
> Position Aware Services on page 20
> Positioning Heatmaps on page 49

Analytics Profile Settings

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

> **Note**
> Supported on AP39xx, AP3xx, AP4xx, and AP5xx.

IPFIX reporting is directed through Extreme Campus Controller.

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

> Add or Edit a Configuration Profile on page 95

RTLS Settings

A Real-Time Location System (RTLS) profile must be configured and enabled within Extreme Campus Controller before Extreme Campus Controller will communicate with the location-based server and before the APs will perform location-based functionality. Extreme Campus Controller 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.
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 Extreme Campus Controller with the same location-based service.
- An RTLS profile cannot be deleted when it is part of an active configuration profile.

Related Topics

Advanced Configuration Profile Settings

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

Table 39: 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 5 GHz band. To make use of Band Steering, ensure that networks are assigned to both radios. For Band Steering to work effectively, configure similar coverage areas for the 2.4 GHz and 5 GHz bands. Design the network for both 5 GHz and 2.4 GHz coverage. For networks where coverage quality differs between bands, disable Band Steering. Enable or disable Band Steering 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	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 & 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.
Session Persistence	Determines if session persistence is enabled. A persistent session directs a client's requests to the same backend server for the duration of a session or the time it takes to complete a task or transaction. Enable this option to improve request response times. For more information, see Session Persistence on page 127.

Table 39: Advanced Configuration Profile Settings (continued)

Field	Description
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 Extreme Campus Controller on WLANs where Extreme Campus Controller is not required. You can override the configuration Profile setting for one or more individual APs 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 configuration Profile 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. Standard size is 1500 bytes. Extreme Campus Controller now supports up to 1800 bytes. This enhancement facilitates the transport of MU-DATA specifically between the AP and the appliance (or between the AP and a switch for VxLAN deployments) without incurring fragmentation. You can override the configuration Profile setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
Scan Mode	**Note:** Supported on AP3xx, AP4xx, and AP5xx models. Determines which channels are scanned. Valid values are: • Default Scan. — Scans all supported channels. Optimized to scan widest possible channel. • Channel Lock — Scans on single channel. • Custom Scan — Scan is based on a selected custom list. Define a custom channel list including channel width. ◦ Radio 1 channels are 2.4G (AP510i/e includes 5G channels). ◦ Radio 2 channels are 5G.
Scan Channels	Select channels for a custom channel list used for **Custom Scan** Scan Mode.

Table 39: Advanced Configuration Profile Settings (continued)

Field	Description

GE2 Port Function	Specify the function of the second AP Ethernet port:
	• Client. Indicates that the client port is enabled on the AP. The client option is used in the following scenarios:
	  ◦ When an AP radio is configured as a Client Bridge. Extreme Campus Controller automatically sets the GE2 port to **Client** when Client Bridge is configured.
	  ◦ To leverage the second port of the access point as a Client port, allowing pass-through access to attached clients. Client access is subject to policy. This capability is also utilized in support of work group meshing. A GE2 Client port is supported on the following access points:
	    ▪ AP3xx, AP4xx, and AP5xx
	    ▪ AP3965
	
	 When the GE2 Port is set to **Client**, the WLAN assignment dialog displays an option to specify the GE2 assignment, and the **Wired Ports** tab is available from the AP Profile.
	• AP Ethernet port traffic backup (fail over) between GE1 and GE2
	• LAG (Link Aggregation Group)
	
	 Link aggregation combines network connections to increase throughput and to provide redundancy in case of link failure. Requires that both ports negotiate to the same speed (1 Gbps).
	
	 Note: LAG is supported on ExtremeWireless AP39xx and 11ax APs in a Centralized site.
	
	 You can override the configuration Profile setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP.

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.

Table 39: Advanced Configuration Profile Settings (continued)

Field	Description
Poll Timeout	Specifies the amount of time, in seconds, to wait for a response from the appliance before rebooting. The value range is from 3 to 600 unless the controller is in an availability pair without fast failover enabled. The default value is 3. **Note:** When configuring a Mesh network, we recommend a value of at least 60 for the non-root AP configuration. Also, it is a best practice to wait at least 60 seconds before applying configuration changes that are applicable to non-root (node) access points. This ensures that possible interruptions due to configuration changes are resolved. You can override the configuration Profile setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
FA Auth Key	Configure custom Fabric Attach Authentication Keys up to 32 characters in length. Extreme Networks products offer a default FA AUTHENTICATION-KEY built-in. You can also configure a custom key here. When a custom key is not configured, the default key is used. The following special characters are *not* supported: {? <tab> \ " ` } You can override the configuration Profile setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP. **Note:** Supported on AP39xx, AP3xx, AP4xx, and AP5xx access points.
LED Status	The LED Status pattern can indicate that the configuration profile has been pushed to the destination appliance. Select an LED Status. Valid values are: **Off** 　LEDs do not light. **Normal** 　Default mode for all APs. Identifies the AP status during the following processes: 　• registration 　• power on 　• boot 　• For APs in a Centralized mode, LEDs are lit solidly. **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 AP3xx, AP4xx, and AP5xx. You can override the configuration Profile setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP.

Table 39: Advanced Configuration Profile Settings (continued)

Field	Description
PEAP User Name and Password	Ability to configure the PEAP (Protected Extensible Authentication Protocol) user name and password for all devices in a device group or for a specific device override. Used to per-provision devices for authorization to connect to the network. Credential and Certificate installation procedures are supported for Wi-Fi 6 APs, AP39xx series APs, and the SA201 Adapter. You can override the configuration Profile setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
Enforce Manufacturing Certificate	Enforce usage of Extreme PKI (Public Key Infrastructure) when establishing an IKE (Internet Key Exchange) tunnel. Both APs and controllers have Extreme CA certificates installed. When this setting is enabled, the controller accepts only APs that provide Extreme PKI. **Note:** Supported on the Defender Adapter SA201 and on the ExtremeWireless access point models: AP39xx, AP3xx, AP4xx, and AP5xx. There must be successful mutual authentication between the AP and the controller. If either side of the authentication fails, the tunnel is rejected. When this setting is enabled, APs that are not PKI capable (self-signed certificates) *are not* able to connect to the controller. The default is to clear this option. When this setting is cleared, the controller accepts the AP with a self-signed certificate. With either type of certificate, the certificate type must match in both directions before the authenticated tunnel is established. Authentication failure messages are logged in the Extreme Campus Controller Events Log. You can override the configuration Profile 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 Extreme Campus 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 180. When using 802.1x, if none of the appliances are available, then likely there is no

path-to-authentication and new clients will be unable to authenticate on the wireless network. If the network association is set to OPEN or PSK SSIDs, no authentication is required and the AP will associate the device based on the 'Default Non-Auth' Role setting configured for the network.

Configuring RF Management

RF Management profiles are AP model dependent and reusable. Default profiles are intended to make RF Management easy, getting you up and running without having to configure an RF policy. However, you can always create additional profiles based off of default RF Management profiles. The RF Management support is dependent on the AP model.

The following AP models are supported:

- AP39xx supporting ACS Policy for RF Management
- AP3xx, AP4xx, and AP5xx supporting Smart RF Policy for RF Management

Related Topics

Configuring ACS RF Policy on page 132

Configuring Smart RF Policy on page 133

Basic RF Management Settings

From the **Basic** tab, set the RF Management policy for both ACS and Smart RF. Select **Smart Monitoring Enabled** to display the Smart RF settings.

Table 40: Basic RF Management Settings

Field	Description
Name	Name of the RF Management policy.
Smart Monitoring Enabled	When enabled, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation. Smart Monitoring is enabled by default. When Smart Monitoring is disabled, the following RF Management tabs are not displayed: **Scanning**, **Recovery**, and **Select Shutdown**. And the following settings are not displayed on the **Basic Settings** page: Sensitivity and Recovery options.

Table 40: Basic RF Management Settings (continued)

Field	Description
Sensitivity **Note:** Available for Smart RF policy only.	Determines pre-defined thresholds for Smart RF. Valid values are: • Low — Interference recovery 30 dBm. Coverage Hole Recovery 20 dBm • Medium — Interference recovery 20 dBm. Coverage Hole Recovery 20 dBm • High — Interference recovery 5 dBm. Coverage Hole Recovery 20 dBm • Custom. Select **Custom** to modify Smart RF settings. **Note:** If the sensitivity setting is too low, you may be tolerating channel congestion, impacting network performance. If the sensitivity setting is too high, you may have difficulty finding an optimal channel. The default Smart RF policy that is delivered with Extreme Campus Controller is configured with **Medium** sensitivity.
Interference Recovery	Determines optimum channel due to noise thresholds, client count and other factors that influence channel switching algorithms. To avoid channel flapping, a defined hold-timer disables interference avoidance for a specific period of time upon detection. Interference Recovery is enabled for the default Smart RF policy.
Coverage Hole Recovery **Note:** Available for Smart RF policy only.	Determines radio power adjustments to react to holes in RF coverage in an AP deployment area. Smart RF determines the radio power adjustments required based on a reporting client's signal to noise (SNR) ratio. If a client's SNR is above the administrator threshold, the connected AP's transmit power increases until the noise rate falls below the threshold. Coverage Hole Recovery is enabled for the default Smart RF policy.
Neighbor Recovery	Determines coverage behavior when a radio failure is detected within the coverage area. RF Management provides automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Neighbor recovery is enabled for the default Smart RF policy.

Select the **Channel and Power** tab to modify radio channel and power settings.

Related Topics

Channel and Power Settings

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 Extreme Campus Controller.

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

Table 41: Channel and Power Settings

Field	Description
Channel Width	Determines the channel width used by the channel on the selected radio. The channel width is set for all APs in a device group. Available options include: • 20 MHz • 40 MHz • 80 MHz (supported on 5GHz only 802.11ac and 802.11ax) • 160 MHz (supported on 5GHz only 802.11ax) • Automatic – Channel width is calculated automatically. This is the default value. **Best Practice:** Operating a 40MHz channel in a 2.4 GHz band can cause co-channel inference with access points in the vicinity. The 2.4 GHz band has limited available channels. Therefore, for proper channel isolation, a 2.4 GHz band allows 3-4 (region dependent) 20 MHz channels. Best practice is to configure a 40MHz channel on a 5 GHz radio.
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 130.

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, select one of the following:
  - ◦ All channels — ACS or Smart RF scans all channels for an operating channel and, when ACS or Smart RF is triggered, the optimal channel is selected from all available channels.

    This plan includes the following channels: 36, 40, 44, 48, 52, 56, 60, 64, 100,104,108,112, 116, 132, 136, 140,144, 149, 153, 157,161, 165.
  - ◦ All Non-DFS Channels — ACS or Smart RF scans all non-DFS channels for an operating channel. The AP selects the best non-DFS channel.

    This plan includes the following channels: 36, 40, 44, 48, 149, 153, 157, 161, 165.
  - ◦ Custom — To configure individual channels from which to select an operating channel, select **Configure**. The **Custom Channel Plan** dialog displays. Select the individual channels you want to include in the channel plan. To select contiguous channels, use the Shift key. To select multiple, non-contiguous channels in the list, use the CTRL key. Select **OK** to save the configuration.
  - ◦ Extended Channel with Weather— ACS or Smart RF selects the best channel from the available channels list. Selected channel may be DFS, weather-radar DFS or non-DFS. Weather-radar channels are approved for selected AP models in selected countries. Consult the compliance information for the selected AP.
    - ▪ This plan includes the following channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120,124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165.
    - ▪ The weather channel includes 5600-5650MHz sub-bands and requires a listening period before the AP can provide wireless service. During the listening period, the Current Channel field for DFS channels displays the value *DFS Timeout*, and the weather channel fields display *DFS Timeout* . In Europe, the listening period can be up to 10 minutes. In the U.S., this period is 1 minute.
- For 2.4 GHz Radio nodes, select one of the following:
  - ◦ 3 Channel Plan — ACS scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in the rest of the world.
  - ◦ 4 Channel Plan — ACS scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world.
  - ◦ Auto — ACS scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world.
  - ◦ Custom — If you want to configure individual channels from which the ACS or Smart RF selects an operating channel, select **Configure**. The **Add Channels** dialog is displayed. Select the individual channels you want to add to the channel plan while pressing the CTRL key, and then select **OK**.

> **Note**
>
> For a list of channels that are included in the selected channel plan, select 🛈 on the user interface.

Related Topics

Configuring ACS RF Policy

The Extreme Campus Controller RF Management policy depends on your AP model. AP39xx access points support Automatic Channel Selection (ACS) as the RF Management policy. Extreme Campus Controller is installed with a default ACS policy.

A Centralized site can support multiple ACS RF policies. Different AP device groups can use different ACS RF policies. You can modify the default policy or create a new policy. Policies that are being used by a device group cannot be deleted, but if the policy is not being used, you can delete it.

To configure ACS:

1. Go to **Configure** > **Sites** and select a Centralized site.
2. Click **Device Groups** tab.
3. Select a device group or click **Add**.

   The **RF Management** value is ACS for AP39xx.
4. Select ✎ next to RF Management, to edit the ACS policy.

> **Note**
>
> After modifying the default ACS policy settings, if you need to return to the initial settings, create a new ACS policy. New policies are comprised of the ACS settings that are delivered with the initial installation. Click ⟳ to create a new policy.

> **Note**
>
> Interference Recovery and Neighbor Recovery should be enabled to allow ACS RF Policy to adjust/change channels automatically. You can use Interference Recovery only, or Neighbor Recovery only.

Related Topics

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 42: ACS Interference Recovery Settings

Field	Description
Channel Occupancy Threshold %	Defines the channel utilization level, measured as a percentage. If the threshold is exceeded, ACS scans for a new operating channel for the AP.
Noise Threshold (dBm)	Defines the noise interference limit, measured in dBm. If the noise interface exceeds this threshold, ACS scans for a new operating channel for the AP.
Update Period (Minutes)	Defines a period of time, in minutes, where the average values for DCS Noise and Channel Occupancy are measured. If the average value for either setting exceeds the defined threshold for that setting, then the AP triggers Automatic Channel Scan (ACS).
Wait Time (Seconds)	Length of the delay (in seconds) before logging an alarm. Default setting is 10 seconds.
Detect Bluetooth	Enable this setting to detect Bluetooth interference on the operating channel.
Detect Constant Wave	Enable this setting to detect Constant Wave interference on the operating channel.
Detect Cordless Phones	Enable this setting to detect cordless phone interference on the operating channel.
Detect Microwaves	Enable this setting to detect microwave interference on the operating channel.
Detect Video Bridges	Enable this setting to detect video bridge interference on the operating channel.

Configuring Smart RF Policy

The Extreme Campus Controller RF Management policy depends on your AP model. AP4xx and AP5xx support Smart RF as the RF Management policy. Extreme Campus Controller is installed with a default Smart RF policy.

You can modify the default policy or create a new policy. Policies that are being used by a device group cannot be deleted, but if the policy is not being used, you can delete it.

> **Note**
> AP3xx, AP4xx, and AP5xx support Smart RF. Only one Smart RF Policy can be used per site.

To configure Smart RF:

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

    The **RF Management** value is Smart RF for AP3xx, AP4xx, and AP5xx.
4. Select ✎ next to RF Management, to edit the Smart RF policy.

Extreme Campus Controller is installed with a default Smart RF policy. You can modify the default policy or create a new policy, but you cannot delete a Smart RF policy.

> **Note**
>
> After modifying the default RF policy settings, if you need to return to the Extreme Campus Controller initial settings, create a new Smart RF policy. New policies are comprised of the Smart RF settings that are delivered with the initial Extreme Campus Controller installation.
>
> Select ⊕ 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. 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 43: AP Scan Settings

Field	Description
OCS Monitoring Awareness Override	Overrides OCS scanning. Smart RF relies on Off-Channel Scanning (OCS) to monitor the RF environment in real-time, allowing managed radios to adapt to changes in the RF environment. OCS can negatively impact some devices. When enabled, OCS checks for sensitive clients (for example, Voice and Power Save clients). If sensitive clients are found, OCS is skipped, and the **Number of Threshold Awareness Hits** counter is incremented.
Number of Threshold Awareness Hits	Enabled 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.

Table 43: AP Scan Settings (continued)

Field	Description
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	The number of samples that each Smart RF managed radio takes before reporting to Extreme Campus Controller. The default is 5 samples from a 5GHz radio and 10 samples from a 2.4 GHz radio when Medium sensitivity is selected.
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 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 44: 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 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 45: 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 46: 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

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 22.

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 Extreme Campus Controller. Upon import, the AP place holder icon displays ().

You may want to create a floor plan before you have the APs installed. Or you may be reusing a floor plan that incorporated different APs from those that you are using now. In either case, the APs are unknown to Extreme Campus Controller.

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

1. From the floor plan **Configure** page, select **Import** and select the floor plan file to import.

   The map is displayed with unknown AP icons ![icon].

2. From the map, right-click each icon ![icon] and select the serial number for the AP that will be installed in that location.

   > **Note**
   >
   > The list of available APs is populated from the selected device groups.

3. To edit the AP placement, select the AP selector ➤ next to the **Place APs** field, then select the AP icon and drag it to a new location.

Related Topics

Add a New Floor Plan

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 22.

.

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 142.

Related Topics

Floor Plan Settings

1. Configure the following parameters for a floor plan.

Table 47: 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 141

Importing or Exporting a Floor Plan on page 142

Importing or Exporting a Floor Plan

Extreme Campus Controller supports the following floor plan file formats:

- Zip
- Extreme Campus Controller
- Ekahau

To import or export a floor plan file, take the following steps:

1. Go to **Configure** > **Sites**. Add a new site or select a site and 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).
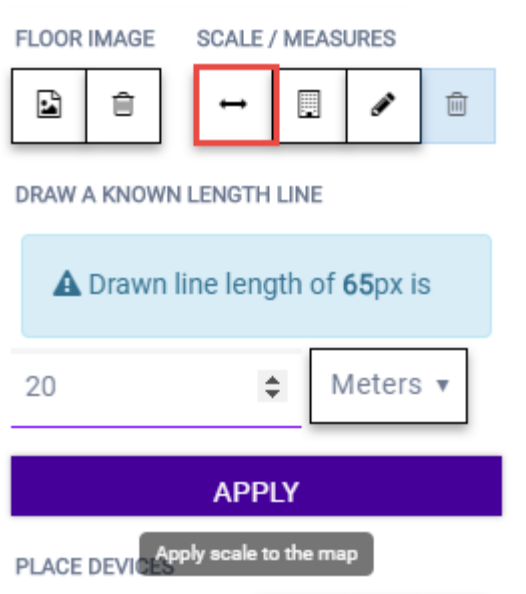
Figure 30: Setting Floor Plan Scale

- 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 145.

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 41

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 🗑.

Advanced Tab

On the **Advanced** tab, you can configure advanced settings for a site:

- **SNMP**. Simple Network Management Protocol configuration for switches associated with a specific site. For more information, see SNMP Configuration on page 312.
- **Preferred Connection**. Control the distribution of APs in a particular site between appliances in a High Availability Pair.

Extreme Campus Controller supports the ability to specify an appliance adoption preference and to support a High-Availability pair of appliances located in separate data centers. APs assigned to a site will discover the appliance specified in the **Preferred Connection**. The load assignment for the preferred appliance persists. However, you can re-map the AP-to-site preference at any time, to adjust for experience, business needs, or network conditions.

For **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 311.

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 Extreme Campus Controller Release Notes for a list of supported APs and switches.

> **Note**
> Extreme Campus Controller supports Extreme Defender Adapter SA201 for the Defender for IoT solution. For more information on Extreme Defender for IoT, refer to documentation located in the Extreme Networks documentation portal.

Related Topics

Access Points

Go to **Configure** > **Devices** > **Access Points** to add and configure APs in Extreme Campus Controller.

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

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

- 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 50.

Related Topics

Understanding Access Point States on page 52
Access Points List on page 50
Query Builder on page 52
AP Actions on page 150
Add APs on page 154
Add a Site on page 92
Device Groups on page 17
Configuring Column Display on page 24

AP Actions

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

Table 48: AP Actions

Field	Description
Manage Certificates	Manage certificates for selected APs. Possible values are: • **Generate CSR** — Enter the attributes for a Certificate Signing Request that is downloaded once the form is complete. See Generate CSR on page 152. Then, send the .csr file to the certificate authority to be signed and returned as a .cer file. • **Apply Signed Certificate** — Apply a signed certificate to the selected APs. See Apply Signed Certificate on page 153. • **Reset to Default** — Remove applied certificates from the selected APs.
Assign to Site	Assign selected APs to a specific site. The **Assign to Site** dialog displays with available sites and device groups. Select a site and device group; then select **Ok**. Selected APs must share the same model type. Based on the AP model type, device groups and sites are displayed in the "assign to" lists. Use this feature to easily move APs to different supported sites. **Note:** When working with 802.11ax access points that offer dual-mode support, make sure that the correct discovery options are configured for device adoption into the destination site. For more information, see the Extreme Campus Controller Deployment Guide. To add a new site or device group, select ⊕ and configure the parameters. For more information, see Assign to Site on page 178.

Table 48: AP Actions (continued)

Field	Description
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 299. **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

NEW! AP Certificates

Access points can establish a secure tunnel with Extreme Campus Controller using a self-signed or manufacturing certificate. This feature is supported on the Extreme Campus Controller version 5.x licensing model. AP certificates are not used when the connection does not use a secure tunnel, and certificates are not supported with Extreme Campus Controller licenses prior to v5.x.

On Extreme Campus Controller you can generate a unique .csr file for each AP. Then, send the .csr file to the certificate authority to be signed and returned as a unique .cer signed certificate. Another option is to apply a generic certificate (.pfx file) that you export from the certificate authority. Generic .pfx certificates can be applied to more than one AP.

Zip files can contain more than one unique .cer certificate. Extreme Campus Controller applies each certificate to the appropriate AP based on the identifying property: serial number, AP name, or MAC address. The zip file can also contain one generic .pfx file that can be applied to multiple APs. However, uploading a single zipped .cer certificate to multiple APs is not supported. Consider this when selecting more than one AP for certificate management.
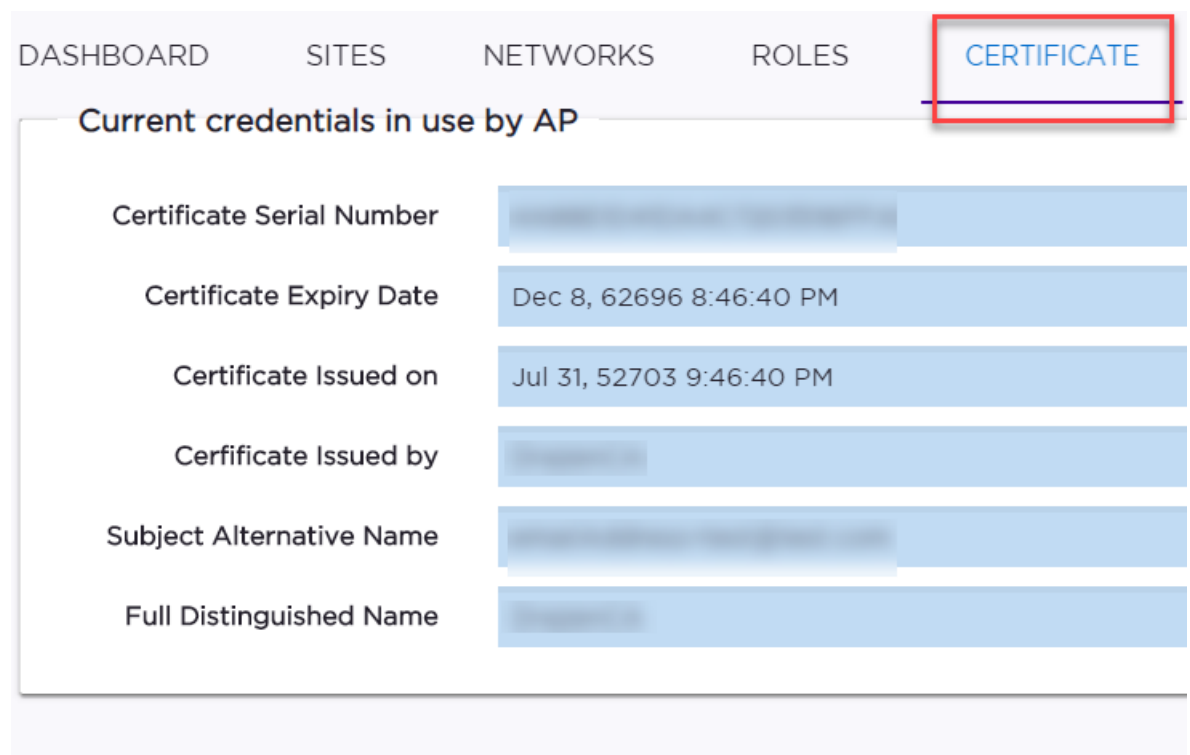
To manage certificates, go to **Configure** > **Devices** > **Access Points**. Select one or more access points and select **AP Actions** > **Manage Certificates**.

From the **Access Point List**, you can verify that a certificate has been applied. Select the **CERT** column for display.

To view certificate details for a selected AP:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP, then select the **Certificate** tab.

   Certificate details display.

Related Topics

NEW! Generate CSR

Complete the following attribute fields to generate a Certificate Signing Request (CSR).

Country Name

Two-letter ISO abbreviation for country name.

State or Province Name

Name of the state or province.

Locality Name

Name of the city or locality.

Organization Name

Name of the organization.

Organizational Unit

Name of unit within the organization.

Common Name

Possible values: AP Name, Serial Number, or MAC address.

Email Address

Email address for notification purposes.

Key Size

The number of bits in the key. This indicates encryption level. Valid values are 1024 or 2048.

Select **Generate CSR**. The certificate file is downloaded to your local machine.

> **Note**
> Send the .csr file to the certificate authority to be signed and returned as a .cer file.

Related Topics

NEW! Apply Signed Certificate

Before you apply a signed certificate, do one of the following:

- Generate a .csr file and send it to the certificate authority to be signed, returning a .cer file.
- Export a generic .pfx certificate from the certificate authority.

To apply a Signed Certificate:

1. (.PFX Only) Provide the password that was used when exporting a .pfx signed certificate from the certificate authority.
2. From the **Upload Signed Certificate** field, drop the certificate file. Or, select the field to navigate to the certificate file. Valid file types are:
   - .pfx
   - .cer (DER Format)

- .zip

> **Note**
> Uploading a single zipped certificate to multiple APs is not supported.

Related Topics

> Generate CSR on page 152
> AP Certificates on page 151
> AP Actions on page 150
> Access Points List on page 50

Add APs

Access points and switches are automatically added to Extreme Campus Controller via the cloud-connector when the DHCP and DNS prerequisites have been met. For full instructions on configuring DHCP, NPS, and DNS services, refer to the *Extreme Campus Controller Deployment Guide* located in the Extreme Networks documentation portal. 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 Extreme Campus Controller, but is not yet a member of a device group, has a status of *In-Service Trouble*.

1. Go to **Configure** > **Devices** > **Access Points**.
2. To add a new AP, select **Add**.
3. To add a clone, select the check box next to an AP in the list and select **Clone**.
4. Configure the following parameters:

    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. Select **OK**.

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

Related Topics

Adoption Rules on page 234

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 154.

Table 49: 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.

Table 49: Radio Properties (continued)

Field	Description
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.
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. The following setting is supported on ExtremeWireless access point models AP3xx, AP4xx, and AP5xx that are configured for a Centralized site. • **Return to configured channel after failed event**. When selected, the device returns to the configured radio channel after a DFS failed event. When this option is enabled, the following options display: ◦ **DFS Revert Hold Time**. The amount of time that a device will stay on a fallback channel before returning to the selected DFS channel. Valid values are 30 to 3600 minutes. The default value is 90 minutes. ◦ **DFS Revert Client Aware**. A threshold that determines if the radio will revert back to the DFS channel after moving to the configured channel. In addition to **DFS Revert Hold Time**, the radio client count also has to drop below the configured threshold. If the number of clients using the radio channel is less than the configured threshold, the radio will revert to the DFS channel. Valid values are 1 – 255. The default value is 0. Zero indicates that the conditioning based on number of clients is ignored.

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.

The following AP models are supported:
- AP39xx supporting ACS Policy for RF Management

- AP3xx, AP4xx, and AP5xx supporting Smart RF Policy for RF Management

Related Topics

Configuring ACS RF Policy on page 132

Configuring Smart RF Policy on page 133

Advanced AP Settings

Table 50: 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	Extreme Campus Controller collects information from the AP, including logs and crash reports if applicable.
Download Trace	Download the trace report.

Related Topics

Advanced Setting Overrides on page 157

IP Address Assignment on page 164

Advanced Setting Overrides

Many AP properties are configured from the device group configuration Profile, where they apply to all APs in the device group. Override the following settings for a specific AP from the **Advanced** > **Overrides** tab.

Best Practice: For a consistent configuration, a best practice is to configure the APs through the configuration Profile. Overrides are available for unique configuration. However, variances from the configuration Profile can result in APs not receiving general policy changes. Consider configuration Overrides carefully. To determine which APs are configured with overrides, from the **AP List**, display the **Overrides** column. See Access Points List on page 50.

To access the **Overrides** dialog:

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

3. Select **Advanced** > **Overrides**.

Table 51: Advanced AP Setting Overrides

Field	Description
Management VLAN ID Override	Virtual Local Area Network Identifier. Enable VLAN tagging to insert a VLAN ID into a packet header identifying which VLAN the packet belongs to. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for 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.

GE2 Client Port	Specify the function of the second AP Ethernet port:
	• Client. Indicates that the client port is enabled on the AP. The client option is used in the following scenarios:
	  ◦ When an AP radio is configured as a Client Bridge. Extreme Campus Controller automatically sets the GE2 port to **Client** when Client Bridge is configured.
	  ◦ To leverage the second port of the access point as a Client port, allowing pass-through access to attached clients. Client access is subject to policy. This capability is also utilized in support of work group meshing. A GE2 Client port is supported on the following access points:
	    ▪ AP3xx, AP4xx, and AP5xx
	    ▪ AP3965
	
	  When the GE2 Port is set to **Client**, the WLAN assignment dialog displays an option to specify the GE2 assignment, and the **Wired Ports** tab is available from the AP Profile.
	• AP Ethernet port traffic backup (fail over) between GE1 and GE2
	• LAG (Link Aggregation Group)
	
	  Link aggregation combines network connections to increase throughput and to provide redundancy in case of link failure. Requires that both ports negotiate to the same speed (1 Gbps).
	
	  Note: LAG is supported on ExtremeWireless AP39xx and 11ax APs in a Centralized site.

Table 51: 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
	    LEDs do not light.
	
	Normal
	    Default mode for all APs. Identifies the AP status during the following processes:
	    • registration
	    • power on
	    • boot
	
	    • For APs in a Centralized mode, LEDs are lit solidly.
	
	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 AP3xx, AP4xx, and AP5xx.

Table 51: Advanced AP Setting Overrides (continued)

Field	Description
Enabling Manufacturing Certificate	Enforce usage of Extreme PKI (Public Key Infrastructure) when establishing an IKE (Internet Key Exchange) tunnel. Both APs and controllers have Extreme CA certificates installed. When this setting is enabled, the controller accepts only APs that provide Extreme PKI. **Note:** Supported on the Defender Adapter SA201 and on the ExtremeWireless access point models: AP39xx, AP3xx, AP4xx, and AP5xx. There must be successful mutual authentication between the AP and the controller. If either side of the authentication fails, the tunnel is rejected. When this setting is enabled, APs that are not PKI capable (self-signed certificates) *are not* able to connect to the controller. The default is to clear this option. When this setting is cleared, the controller accepts the AP with a self-signed certificate. With either type of certificate, the certificate type must match in both directions before the authenticated tunnel is established. Authentication failure messages are logged in the Extreme Campus Controller Events Log. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for one or more individual APs from here.
Poll Timeout	Specifies the amount of time, in seconds, to wait for a response from the appliance before rebooting. The value range is from 3 to 600 unless the controller is in an availability pair without fast failover enabled. The default value is 3. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for one or more individual APs from here.
FA Auth Key	Configure custom Fabric Attach Authentication Keys up to 32 characters in length. Extreme Networks products offer a default FA AUTHENTICATION-KEY built-in. You can also configure a custom key here. When a custom key is not configured, the default key is used. The following special characters are *not* supported: {? <tab> \ " ` } **Note:** Supported on AP3xx, AP4xx, and AP5xx models. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for one or more individual APs from here.

Table 51: Advanced AP Setting Overrides (continued)

Field	Description
IBeacon Settings	IBeacon is supported on the following access point models: • AP3xx • AP4xx • AP5xx • 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.
WLAN	You can override the radio WLAN assignments for a specific AP. The result is that the AP has a unique radio WLAN assignment, plus port and IOT assignments, and policy definitions that are defined in the configuration Profile. The AP must be part of a device group, but you can override the WLAN per AP in order to enable or disable a selected network. This can be useful for testing and troubleshooting purposes. See WLAN Override on page 162.
PEAP User Name and Password	Ability to configure the PEAP (Protected Extensible Authentication Protocol) user name and password for all devices in a device group or for a specific device override. Used to per-provision devices for authorization to connect to the network. Credential and Certificate installation procedures are supported for Wi-Fi 6 APs, AP39xx series APs, and the SA201 Adapter.
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

WLAN Override

A configuration Profile is specified at the device group. All access points that are part of the device group are associated with the same configuration Profile. The network policies are created based on default policies defined for the WLAN, and policies added directly to the configuration Profile. The AP has all WLAN and policy assignments based on the corresponding Profile.

You can override the radio WLAN assignments for a specific AP. The result is that the AP has a unique radio WLAN assignment, plus port and IOT assignments, and policy definitions that are defined in the configuration Profile. The AP must be part of a device group, but you can override the WLAN per AP in order to enable or disable a selected network. This can be useful for testing and troubleshooting purposes.

> **Note**
> Extreme Campus Controller will display a warning if the network reassignment affects the primary BSSID on the radios, resulting in a radio reset. You will have the opportunity to consider the impact of network reassignment before overriding a WLAN.

Extreme Campus Controller automatically determines the related role assignments that are referred by the new WLAN service, and it adjusts the role listing per AP. Roles assigned to the Profile and roles referenced by the new WLAN Service are merged. The larger role set is visible per AP for diagnostic purposes.

To override the WLAN assignment:

1. On the **Overrides** tab, select **WLAN**, and then select **Configure**.

   Extreme Campus Controller displays a list of configured networks. The settings that display are those that are inherited from the associated configuration Profile.
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 5 GHz band. To make use of Band Steering, ensure that networks are assigned to both radios.

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

Band Steering requires that the same SSID be present on both 2.4 GHz and 5 GHz radios. Extreme Campus Controller automatically collapses radio assignments to a single selection when Band Steering is enabled, and a single, dual-band radio is represented for WLAN service override assignment. Adding a WLAN service automatically creates an assignment to both radios (2.4 GHz and 5 GHz). You can disable Band Steering at either the AP override or 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

NEW! Cell Size Control Settings

These AP settings help improve network connectivity. They can be set at the device group level or as an AP Override setting.

Table 52: Cell Size Control Settings

Field	Description
Probe Suppression on Low RSS	Reduces the number of probe responses by preventing clients with low RSS from associating with an AP radio. This setting is configured per radio. Clients with RSS measured below the Probe Suppression RSS Threshold will not associate with the AP. This setting is disabled by default.
Disassociate on Low RSS	This setting is supported on AP39xx, AP3xx, AP4xx, or AP5xx, (in a Centralized Site). It is always disabled by default. This setting forces clients with low RSS to disassociate from an AP radio. This setting is configured per radio. A client is forced off an AP radio when RSS is measured at 5dBm below the Probe Suppression RSS Threshold. Enabling this option forces a client to roam to a better AP for improved network performance.
Probe Suppression RSS Threshold (dBm)	This setting is available when **Probe Suppression on Low RSS** is enabled. This setting determines the RSS threshold for forced disassociation and probe suppression. The default threshold is -90 dBm. Valid value range is -50dBm to -100dBm. **Best Practice:** Probe Suppression Threshold should not be greater than -70dB. The Probe Suppression Threshold defines the signal strength value that is deemed too low to be acknowledged by the AP. Setting the threshold above -70dB can result in an AP not acknowledging clients in close proximity, leading to poor connectivity or a sub-optimal roaming experience. The best practice is to follow the Site Survey methodology to determine the best value for the AP installation.
Probe Response Retry Limit	The default Probe Response Retry Limit is 4. If devices are having a problem connecting to the network, due to congestion or due to the quality of the device, consider increasing the retry limit. Maximum value is 10.
Rx Sensitivity Reduction (dB)	New APs are very sensitive and can pick up unwanted channel interference. If this is an issue, add an offset of 5-10 dB, which will reduce signal sensitivity and improve signal quality.

Related Topics

IP Address Assignment

Table 53: 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 Extreme Campus Controller Deployment Guide.
Static	Indicates if a permanent IP address is assigned for this AP. After selecting **Static**, provide the information for the following address fields: • IP Address • Mask — Subnet Mask • Default Gateway

Related Topics

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.

> **Note**
>
> Single-band antennas limit the AP operation to the radio that is associated with the antenna and reduce the sensor functionality of the IoT sensor radio.

Professional install

Radio 1/2 Port 2.4G/5G-1 Antenna Type   [No Antenna]

Radio 1/2 Port 2.4G/5G-2 Antenna Type   [No Antenna]

IoT Antenna Type   [No Antenna]

Radio 1 Attenuation   [0   ▾]

Radio 2 Attenuation   [0   ▾]

Figure 31: Professional Install Settings (Two port AP)

Related Topics

AP310e/AP360e Professional Install Settings

The following rules apply to AP310e and AP360e antenna installation:

- Group 1 (2.4 GHz/5 GHz) accepts identical dual-band antennas.
- Group 2 (5 GHz) accepts identical 5 GHz or dual-band antennas.
- Antennas must be configured consecutively for each group. Group 1 starts with Port 1/Group 1 and Group 2 starts with Port 3/Group 2. An equal number of antennas must be configured for both groups. For example, to support a 2x2 deployment, install Group 1 and Group 2 — 2 antennas each.
- Mode 1. Radios 1 and 2 are enabled when:
    - Both groups of antennas must be configured. Radio 1 is enabled only if one or more antennas are configured in Group 1. Radio 2 is enabled only if one or more antennas are configured in Group 2.
- Mode 2. Radio 1 is a 2.4/5 GHz sensor and Radio 2 forwards traffic.
    - Radio 1 dual-band sensor is enabled only if one or more antennas are configured in Group 1.

- ◦ Radio 2 5 GHz WLAN service is enabled only if one or more antennas are configured in Group 2.
- Mode 3. Radios are configured Dual 5 GHz mode.
  - ◦ Radio 1 is enabled only if one or more antennas are configured in Group 1.
  - ◦ Radio 2 is enabled only if one or more antennas are configured in Group 2.

Table 54: Radio Modes AP310e/AP360e

Mode	Radio 1	Radio 2
1	2.4 GHz traffic forwarder	5 GHz traffic forwarder
2	2.4 GHz/5 GHz sensor	5 GHz traffic forwarder
3	5 GHz traffic forwarder (channels 36-64)	5 GHz traffic forwarder (channels 100-165)
Sensor	2.4 GHz sensor	5 GHz sensor

Figure 32: AP310e/AP360e Antenna Professional Install

Related Topics

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 33: AP410e Professional Install Settings

Related Topics

AP460e Professional Install Settings

The AP460e is an outdoor AP with external antennas. The AP460e has the following antenna layout:

- Radio 1 uses ports 5 and 6
- Radio 2 uses ports 1 through 4
- Radio 3 uses ports 7 and 8
- IoT radio uses port 9 (not configurable)

The default value for Radios 1-3 is "No Antenna", and the default value for the IoT radio is "Internal."

The ports are grouped as follows. Each port in the group must be configured with the same antenna model:

- Group 1 — Ports 1 through 4 (Radio 2)
- Group 2 — Ports 5 and 6 (Radio 1)

- Group 3 — Ports 7 and 8 (Radio 3)

> **Note**
> To display the **Professional Install** dialog, the AP must be part of an AP460e device group.

Figure 34: AP460e Professional Install Settings

Related Topics

Add APs on page 154

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 35: AP510e Antenna Professional Install

Related Topics

Switches Configure

AP560h Professional Install

The AP560h is an outdoor AP that has two types of selectable, internal antenna. Select one of the following antennas:

- INTERNAL-560H-30, dual band, 8feed, 30 degree sector. This is the default antenna.
- INTERNAL-560H-70, dual band, 8feed, 70 degree sector

> **Note**
> The AP must be part of an AP560 device group to display the **Professional Install** dialog.
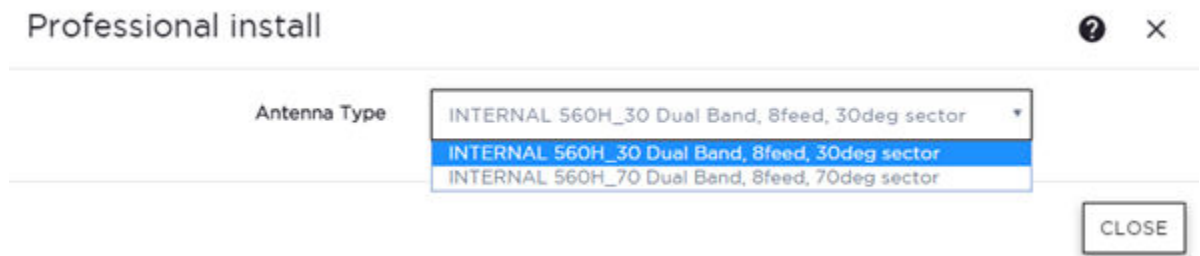

Figure 36: AP560h Professional Install Settings

Related Topics

Add APs on page 154

Switches

Extreme Campus Controller can manage a maximum of 1000 switches.

- To configure a switch, go to **Configure** > **Devices** > **Switches**.
- For a list of supported switches, see the Release Notes.

Related Topics

Adding a Switch on page 171

Configure a Switch on page 173

Switch Actions on page 170

Switches List on page 72

RADIUS Configuration for Switches Per Site on page 93

Switch Actions

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

Table 55: 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.

170 Extreme Campus Controller User Guide for version 5.16.03

Table 55: Switch Actions (continued)

Field	Description
Upgrade	Upgrade switch software. You must be an Administrator to upload the per-packaged software.
Retrieve Traces	Initiates a traces routine creating a zip file that includes switch configuration, state information, and log files. Extreme Campus Controller receives the Traces zip file and presents a download-able zip file in the Traces tab on the Monitor page for the switch. Extreme Campus Controller keeps one file and overwrites that file as subsequent files are received.
Assigned to Site	Assign selected switches to a site. **Assign to Site** dialog displays with available sites. Check one site and click **Ok**.

Related Topics

Understanding Switch States

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

Table 56: 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 Extreme Campus Controller • Configuration is pending acknowledgment from switch • Switch reset pending • Switch reboot pending • Switch upgrade pending
⚫	Unknown. Switch has not discovered the Extreme Campus Controller.
🟥	Critical: • Switch stops sending requests for 5 minutes or longer • Consistent with a lost of connectivity to Extreme Campus Controller

Adding a Switch

Access Points and Switches are automatically added to via the cloud-connector when the DHCP and DNS prerequisites have been met. You can use the Add functionality to pre-provision any AP or switch before they connect.

To add a switch to your network:

1. Per-configure your external DHCP and DNS servers on your network for discovery of the new switch. In order for the to communicate to the Extreme Campus Controller:

    *   The DHCP Server (that will be serving an IP to the switch) needs to return a DNS Server and Domain Name to the switch.
    *   The DNS Server needs to map the name `extremecontrol.<domain-name>` to the IP address of the Extreme Campus Controller that you plan to add the switch.
    *   Confirm that the DHCP server is serving the correct DNS and domain name information.

    > **Note**
    >
    > For full instructions on configuring DHCP, NPS, and DNS services, refer to the *Extreme Campus Controller Deployment Guide* located in the Extreme Networks documentation portal

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 170.

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 178.

> **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, Extreme Campus Controller displays a list of ports on the **Switch Configuration** page. From the configuration page, create LAG groups and select the Admin state, Port Function, and PoE of each port.

   For each port, the following information is displayed:
   - Admin State
   - Name
   - Alias Function
   - Speed
   - Neighbor
   - LAG Members
   - PoE

2. Select one or more ports from the list. Then, set the Admin State, Port Function, and PoE options to **On** or **Off**. Select **Apply** after each selection.

Switch in CLI-Mode:

After placing an ExtremeXOS switch in CLI-Mode, the **Switch Configuration** page display is limited to the following buttons:

- **Activate Console**. Opens a remote console for a live SSH console session.
- **Backups**. Displays a list of switch configuration backup files. From this list you can view a file or restore a configuration from a backup file.
- **Create Backup**. Create a backup file of the switch configuration.
- **Advanced**. In CLI-Mode, switch advanced settings are limited to changing the switch mode. From here you can select **Change to GUI-Mode**.

Related Topics

LAG Configuration

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

Switch Port Configuration

To access port configuration:

1. Go to **Configure** > **Devices** > **Switches**.
2. Select a switch.
3. Select a port in the **Name** column.

Configure the following parameters for individual switch ports:

Name

Port name.

Alias

(Optional) A user-friendly name used as an alias for the port.

Admin State

Indicates if the port is an Admin Port. Valid values are On or Off.

Function

Port function refers to the type of device the port serves. Valid values include:
- Access Point. Connects an access point. This port is part of all VLANs that are defined for all VLANs on the site.
- Interswitch. Serves as a point to point link to another switch. This port is part of all VLANs that are defined for all VLANs on the site.
- Host. Connects to a host, such as a workstation, phone, or printer.
- Other. Any other type of switch connection.

For Host and Other ports, specify the following:
- VLAN ID and PVID (port VLAN ID)
- Tagged status

- Authentication mode
- MAC-based Authentication (MBA)

> **Note**
> Configure only one untagged VLAN ID /PVID per port.

PoE Enabled

Indicates if the port is enabled for Power over Ethernet. PoE must be supported on the port.

VLANs

Select one or more configured VLANs. Click the plus sign to add the VLAN to the list.

Authentication Mode

Authentication Mode. 802.1x can be configured on individual ports. When Authentication is enabled on the switch port, this switch gets the RADIUS Authentication definition and the RADIUS servers specified under the site configuration are used.

- 802.1x
- Disabled

MAC-based Authentication (MBA)

MAC-based Authentication (MBA) option displays and is automatically enabled when Authentication mode above is **Disabled**.

When Authentication mode is disabled, MBA can be configured on individual ports. When MBA is enabled on the switch port, the switch gets the RADIUS Authentication definition and the RADIUS servers that are specified under the site configuration are used.

Related Topics

RADIUS Configuration for Switches Per Site on page 93

Advanced Switch Settings

Table 57: 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 Extreme Campus Controller. • Interswitch — All tagged and untagged VLANS are configured for all AP device groups that are serviced by the switch, along with all of the VLANS used by the host and other port types.

Table 57: Advanced Switch Settings (continued)

Field	Description
SNMP Configuration	You can configure SNMP for the individual switch or for the full Extreme Campus Controller. For more information, see SNMP Configuration on page 312.
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 75. • 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 157

IP Address Assignment on page 164

Access the Switch CLI

Extreme Campus Controller allows access to an ExtremeXOS switch CLI for troubleshooting and manual configuration. Switch CLI access is available in two modes:

- GUI-Mode. Provided for troubleshooting using CLI Show commands.

  This is the default mode for the switch. For more information on troubleshooting an ExtremeXOS switch, see Troubleshoot a Switch Using the CLI on page 75.

- 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.
    ◦ Extreme Campus Controller uploads and stores the configuration file in Redis.
  - Switching to GUI-Mode *is* service disrupting:
    ◦ GUI-Mode is the default mode for a switch. When you change to CLI-Mode, and then back to GUI-Mode, the switch is reset to factory settings and configured based on the defaults for the switch model and the site configuration.

To access the switch CLI-Mode:

1. Go to **Configure** > **Devices** > **Switches** and select an ExtremeXOS switch.
2. Select **Advanced**.

3. Select **Change to CLI-Mode**.

4. Select **Activate Console**.

   A console window opens. It can take up to 60 seconds for the switch to connect.

5. When the login prompt displays, log in with your Extreme Campus Controller credentials.

Related Topics

Switch Configuration Backup Files

When a switch is changed to CLI-mode, Extreme Campus Controller automatically creates a backup file of the switch configuration. It also provides an option to create additional configuration backup files. You can create the file, view the file within the user interface, and restore the switch configuration from a backup file.

To access the switch configuration backup files:

1. Activate CLI-Mode on an ExtremeXOS switch. For more information, see Access the Switch CLI on page 177.

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

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

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**.

    Extreme Campus Controller displays a list of devices.

2. Select one or more devices, and then select **Actions** > **Assign to Site**.

    > **Note**
    >
    > Selected APs and adapters must be the same model type.

    The **Assign to Site** dialog opens.

3. Select a site. To create a new site, select ⊕.
4. Select a device group. To create a new device group, select ⊕.

    Refer to the related information for rules associated with creating sites and device groups.

    > **Note**
    >
    > When working with 802.11ax access points that offer dual-mode support, make sure that the correct discovery options are configured for device adoption into the destination site. For more information, see the Extreme Campus Controller 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 58: WLAN Service Configuration Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Maximum 32 characters. Upper and lowercase allowed. Example: PermanentStaff

Hotspot	The following values are valid for hotspot configuration:
	
	• **Disabled**. Hotspot functionality is not enabled. Default value.
	• **Enabled**. Hotspots are enabled for this WLAN.
	  ◦ Privacy is set by default to WPA and Mandatory Frame Protection (MFP) is enable.
	  ◦ The authentication method is set to AAA with External Radius Server. You can configure MBA, if required.
	  ◦ Auth Type is WPA2-Enterprise (802.1x/EAP)
	• **OSU**. Allows the definition of Online Sign Up or OSEN WLAN. When configuring Online Signup for the hotspot, you must configure a separate OSU WLAN. Then, specify that WLAN on the Online Signup tab. Configure the policy and topology assigned to the OSU WLAN to allow access only to the OSU server. No access to the internet. Valid Auth Type values for OSU Hotspot are:
	  ◦ Open
	  ◦ WPA2-Enterprise (802.1x/EAP)
	
	Note: Once you have defined a WLAN service with a hotspot, you cannot disable the hotspot. You can only delete the WLAN service and recreate it.
	
	For more information, see Hotspot on page 189.

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

Table 58: WLAN Service Configuration Settings (continued)

Field	Description
AuthType	Define the authorization type. Valid values are: • Open —Anyone is authorized to use the network. This authorization type has no encryption. The Default Auth role is the only supported policy role. • OWE — Opportunistic Wireless Encryption (OWE) offers security to open networks, ensuring that traffic between an AP and a client is encrypted. Other clients can sniff and record traffic, but cannot decrypt it. • WEP — Static Wired Equivalent Privacy (WEP) offers keys for a selected network, that match the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 networks. Specify one WEP key per network. This option is offered to support legacy APs. See Privacy Settings for WEP on page 186. • 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 185. • WPA2 Enterprise w/ RADIUS — Supports 802.1X authentication with a RADIUS server, using AES encryption. This method can be used with client certificate-based authentication (EAP-TLS). All 802.1X protocols are supported. Two-stage authentication is supported offering a combination of MAC-Based (MBA) authentication and WPA2-Enterprise (802.1x/EAP). The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP). **Note:** Captive Portal is not supported when using WPA2 Enterprise w/ RADIUS. An exception is *Centralized Web Authentication (CWA)*. CWA captive portal supports WPA2 Enterprise w/ RADIUS. See Privacy Settings for WPAv2 Enterprise with RADIUS on page 185. • WPAv3 - Personal with SAE — 128-bit encryption, supported on: ◦ AP3xx running ExtremeWireless WiNG 7.3x and later. ◦ AP4xx running ExtremeWireless WiNG 7.3x and later. ◦ 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

Table 58: WLAN Service Configuration Settings (continued)

Field	Description
	password compromises. See Privacy Settings for WPAv3 with SAE on page 184. • 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 184.
Enable Captive Portal	Check this option to enable captive portal support on the network service.
Captive Portal Type	See Captive Portal Settings on page 200.

MAC-based Authentication	The following parameter displays when MAC-based Authentication is enabled:
	• **MBA Timeout Role**. Select the role that will be assigned to a wireless client during MAC-based authentication (MBA) if the RADIUS server access request times out. If no MBA Timeout Role is selected, then a RADIUS server timeout is treated like an Access-Reject, which prevents the client from accessing the network. Other options:
	  ◦ ⊙ — create a new role
	  ◦ ▰ — edit role
	  ◦ ▢ — delete role
	• Two-stage authentication is supported offering a combination of MAC-Based (MBA) authentication and WPA2-Enterprise (802.1x/EAP). The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP).

Authentication Method	Displayed after **Captive Portal** or **MBA** is selected. Select from the following authentication values: • Default. Select **Configure Default AAA**. • Proxy RADIUS (Failover). Configure up to 4 RADIUS servers for redundancy. • Proxy RADIUS (Load Balance). Configure up to 4 RADIUS servers for load balancing. • Local. Look up in the local password repository. • LDAP. Look up on a remote LDAP server. This option enables LDAP Configuration.

**Table 58: WLAN Service Configuration Settings (continued)**

Field	Description
AAA Policy	Select a AAA policy or select ⊕ to add a new policy. Alternatively, you can select ✎ to edit an existing policy. To see the list of configured AAA policies, go to **Configure** > **AAA Policy**. This option is not displayed for WLAN Networks that do not require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the Extreme Campus Controller. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal. AAA Policy can only be configured for WLAN Networks requiring MACAUTH, External Captive Portal, or EAP.
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 Extreme Campus Controller. Do not authenticate MAC address on the RADIUS server. This setting is not available when you have selected **Default** as the Authentication Method.
Default UnAuth Role	The default network policy roles for an unauthenticated client. Select a role from the list. Other options: • ⊕ — create a new role • ✎ — edit selected role • ☐ — delete selected role
Default Auth Role	The default network policy roles for an authenticated client. Select a role from the list. Other options: • ⊕ — create a new role • ✎ — edit selected role • ☐ — delete selected role Select the policy role as the default authentication policy role. Typically, **Enterprise User** is the Default Auth Role. You can select any of the configured roles. To configure a new role: 1. Go to **Configure** > **Policy** > **Roles**. 2. Go to **Onboard** > **Rules** and edit a policy rule, specifying **Default Auth Role** in the Accept Policy field.

Table 58: WLAN Service Configuration Settings (continued)

Field	Description
Default VLAN	The default network topology. A topology can be thought of as a VLAN (Virtual LAN) with at least one egress port, and optionally include: sets of services, exception filters, and multicast filters. Examples of supported topology modes are Bridged at AP and Bridged at AC. Select a VLAN from the list. Other options: • ⊕ — create a new VLAN • ◪ — edit selected VLAN • ▢ — delete selected VLAN
Scheduling	**Note:** This option is unavailable until you install and run Scheduler for Extreme Campus Controller. Select **Scheduling** to open the Scheduler application. This is a Docker application that resides on Extreme Campus Controller. Download Scheduler for Extreme Campus Controller 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). **Best Practice:** TKIP encryption is considered to be a less secure means of communication. An industry best practice is to use a more secure option for network privacy.
- Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. 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.

Two-stage authentication is supported offering a combination of MAC-Based (MBA) authentication and WPA2-Enterprise (802.1x/EAP). The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP).The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP). Wireless devices must pass both MBA and WPA2-Enterprise before they are allowed access to the network. After passing 2-staged authentication, the wireless client is fully authenticated and assigned a policy role as provisioned by the administrator. If either part of the two-staged authentication process fails, the client is disconnected from the network, and the client must attempt MBA authentication again.

> **Note**
> Captive Portal is not supported when using WPA2 Enterprise w/ RADIUS. An exception is *Centralized Web Authentication (CWA)*. CWA captive portal supports WPA2 Enterprise w/ RADIUS.

Configure the following privacy settings:

- TKIP-CCMP — Select this option to use Temporal Key Integrity Protocol (TKIP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). **Best Practice:** TKIP

encryption is considered to be a less secure means of communication. An industry best practice is to use a more secure option for network privacy.

- Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. PMF adds an integrity check to control packets being sent between the client and the access point. 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

Privacy Settings for WEP

> ➡ **Important**
> Always use a restrictive policy to the associated VLAN to reduce your exposure after a breach.

Static WEP (Wired Equivalent Privacy) uses keys for a selected network, that match the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 networks. Specify one WEP key per network.

> 📝 **Note**
> This option is offered to support legacy APs.

Configure the following privacy settings for a WLAN network:

- WEP Key Length — Select the WEP encryption key length. Valid values are: 64-bit and 128- bit.
- Input Methods — Select one of the following input methods:
  - Input Hex — If you select **Hex**, type the WEP key input in the WEP Key box. The key is generated automatically, based on the input.
  - Input String — If you select **String**, type the secret WEP Key string used for encrypting and decrypting in the WEP Key box.
- Key Index — Select the WEP encryption key index. Valid values are 1 to 4.
- WEP Key — Type the WEP key using the **Input Method** chosen above.

Related Topics

Mesh Point Network

An access point can be configured to be a part of a mesh network. In a mesh network, nodes in the network can communicate with each other, and each node can maintain more than one path to its peers. Mesh networking enables users to access broadband applications anywhere by providing robust, reliable, and redundant connectivity to all the members of the network. When one of the nodes in a mesh network becomes unavailable, the other nodes in the network can still communicate with each other directly or through intermediate nodes.

Mesh provides efficient routing and path changes in infrastructure and mobility modes by proactively maintaining a table of alternative paths to mesh point root APs. Alternative paths allow root APs the flexibility to change paths immediately when a better path becomes available. This proactive approach allows a mesh AP to make intelligent path decisions in a dynamically changing RF environment.

Consider the following about a mesh network:

- 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. In a mesh point network, APs automatically determine the best path to each mesh point root AP. A single hop path is not necessarily better than a path with multiple hops.
- A mesh network is self-healing. The network reforms when an AP fails, preventing a single point of failure.

To create a mesh network:

1. Configure a network mesh point.

   Initially, configure non-root APs over wired Ethernet, connected to the Management Port. If you need to modify the configuration of a non-root AP after deploying in a mesh network, reconnect the AP through the Ethernet port and verify mesh point configuration. When a non-root AP is incorrectly configured in a mesh network, it can become stranded. To recover a stranded AP, reconnect to the Management Port through the wired Ethernet.
2. Create a device group and configuration Profile for the root AP and a second device group and configuration Profile for the non-root APs.
3. From the device group configuration Profile:
   - Specify the Mesh Point Network.
   - Specify Advanced configuration Profile settings.
   - Specify Mesh Point Settings.

     > **Note**
     > The access points are limited to one mesh point.

     > **Note**
     > Mesh Point is supported on ExtremeWireless AP39xx and the Wi-Fi 6 access point models: AP3xx, AP4xx, and AP5xx. The mesh network must contain only AP39xx access points or only Wi-Fi 6 access points. You cannot combine the AP39xx platform with the Wi-Fi 6 access point platforms in a single mesh network.

Related Topics

Configure a Mesh Point Network

1. Configure the mesh point.

   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 **Mesh Points** tab, and select the mesh point network for a single radio.

   > **Note**
   > The access points are limited to one mesh point.

3. Select **Advanced** and configure the device group Profile settings. See Advanced Configuration and Mesh Point Profile Settings on page 98.

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 LAN/WAN and provides a wired backhaul to the network.

Auth Type

A pre-shared key (PSK) is used to AES encrypt traffic traveling between Mesh Point APs. Modifying the key after a non-root AP is deployed may cause it to become stranded. Connect the non-root AP through the Ethernet port before changing the PSK.

Select **Edit Privacy** to enter the WPAv2 key.

Related Topics

Mesh Point Network on page 187

Configure a Mesh Point Network on page 188

Advanced Configuration and Mesh Point Profile Settings on page 98

Mesh Point Network Diagram on page 77

NEW! Hotspot

Extreme Campus Controller supports the definition of Hotspot 2.0 service for AP39xx and Wi-Fi 6 access points deployed in a Centralized site.

Traditionally, using a hotspot presents end users with several challenges, including initial connection issues, security concerns, and connectivity while roaming. Hotspot 2.0 offers the following features to improve the hotspot end-user experience:

- Pre-association network discovery and selection using the dot11u ANQP protocol, resulting in a seamless initial connection.
- Simplified account registration. Network administrators create accounts easily, and provisioning is achieved without user input.
- Enhanced security, using over the air transmission secured by WPAv2.

Each hotspot WLAN has its own Access Network Query Protocol (ANQP) configuration. The HESSID and ANQP Domain ID are specific to the hotspot WLAN.

With pre-association, a mobile device uses ANQP to perform network discovery. The mobile device's connection manager uses hotspot information, such as the service provider policy and user preferences, to automatically select a hotspot network. A mobile device queries the hotspot for key service provider identification and authentication information and selects a network. The ANQP response is generated using parameters configured by the hotspot operator.

Only one hotspot WLAN can be assigned to an AP and to a specific Profile configuration. The hotspot WLAN can refer to a single Online Signup (OSU) WLAN, which can be open or encrypted. Network operators define the filter policy during hotspot configuration.

Related Topics

Configure Hotspot on page 189

NEW! *Configure Hotspot*

To configure a hotspot:

1. Go to **Configure** > **Network** > **WLAN Services** > **Add**.
2. From the Hotspot field, select **Enable**.
   The **Configure** button displays.
3. Select **Configure**.
4. Configure the following settings:
   HESSID

   One SSID can be used across multiple WLANs (BSS), so the HESSID helps a client identify when the BSSID belongs to a homogenous BSS with identical configuration. Beacon with same {HESSID, SSID} pair belong to same WLAN. The {HESSID, SSID} pair must be unique for each WLAN. By default, the HESSID is set to the MAC address of the controller Ethernet port. Hotspots can have the same HESSID as long as the SSID is unique. If opting to configure the HESSID manually, we recommend using an AP BSSID as the HESSID. In a mobility domain, manually configure the HESSID to a unique value, differentiating it from the value used in the controller's WLAN.

   Access Network

   Identifies the type of network. Valid values are:

   - Private network. An enterprise network with user accounts.
   - Private network with guest access. An enterprise network providing guest access.
   - Chargeable public network. (Default) Open to anyone but access requires payment.
   - Free public network. Open network, free of charge but may still require acceptance of terms of use (and may involve OSU servers with captive portal).

   DGAF Disabled

   Downstream Group-Address Forwarding Disabled. By default this option is checked. When checked, the AP is not forwarding downstream group-addressed frames.

   Select each tab to complete the hotspot configuration.

   > **Note**
   > All required fields on the selected tab must be filled out before you can select **OK** to save the configuration.

Related Topics

Hotspot Identification on page 190
SP Identification on page 191
Network Characteristics on page 194
Online Signup on page 196

NEW! *Hotspot Identification*

From the **Hotspot Identification** tab, configure the following parameters:

Domain

FQDN specified by the user. Default value is empty string. This is a list of one or more domain names of the entity operating the hotspot network. Domain names in the domain name list may contain sub-domains. If the service provider's FQDN is not in the domain name list but is in the realm list, then a mobile device that chooses that service provider is considered to be roaming.

Venue Info

Describes the venue. Select from a list of predefined values:

1. In the first field, select a description of the venue group.
2. In the second field, select a value. The second field is not populated with values until after you select a value from the first field. The default value is **Unspecified**.
3. Select **New** to configure:
   - Operator Name
   - Venue Name
   - Language

> **Note**
> Configure up to four languages for each venue.

Figure 37: Hotspot Identification Tab

Related Topics

NEW! *SP Identification*

The hotspot SP Identification tab displays hotspot properties for service provider identification and authentication.

To configure SP Identification for the hotspot:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 189.
2. Select the **SP Identification** tab.

Figure 38: Service Provider Identification

3. Configure the following parameters:

Realm. The the NAI (Network Access Identification) Realms list is a FQDN (Fully-Qualified Domain Name) of the service provider. This is a list of realms that can be successfully authenticated. Each realm may have up to eight supported EAP methods.

To add realms:

a. Select **New**.
b. Enter a value in the **Realm** field. The NAI Realm is a FQDN of the service provider.
c. Select the EAP Method.

Figure 39: Realm Configuration

Configure an NAI Realm list for each hotspot as follows:

* Add all realms that can authenticate the logon credentials or certificate credentials of a mobile device, including the realms of all roaming partners that are accessible from the hotspot AP. Include the realm of the home SP.
* Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information.
* You can configure the EAP method list to support devices that do not know the EAP methods that are being used by a given service provider.

If the device has been provisioned with the home service provider, the device does not need to use the EAP methods in the NAI Realm List. The mobile device knows the EAP method required to authenticate against its home service provider and automatically uses it.

> **Note**
> Keep your DNS server records up to date so that mobile devices can resolve the server domain names (FQDN).

Mobile devices with a SIM or USIM credential, can obtain a realm from the hotspot NAI Realm list. While 3GPP credentials are usually used to access a hotspot, a targeted NAI home query is an

efficient alternative approach. The device's connection manager compares the realm information in the list to the information that is stored on the device. The connection manager uses the mobile device's pre-configured user preferences and policy to make a decision between a hotspot AP or a non-hotspot AP, if both are available.

Roaming Consortium.To configure authentication of mobile devices to the members of a roaming consortium, or to a particular SP that has a roaming consortium, add the appropriate **IEEE-assigned Organizational Identifier (OI)** here. Specify two identifiers unique to the organization that are part of the MAC address.

Use roaming consortium authentication when you do not know all the authenticated realms. Using identifiers unique to the organization in the beacon is a battery efficient roaming method because there are no ANQP queries needed.

3GPP Cellular Network. This is a list of cellular network IDs in the form of mobile country code (MCC), mobile network code (MNC). This list establishes whether an AP has a roaming arrangement with the 3GPP service providers.

   a. Select **New** to expand the **3GPP Cellular Network** pane.

   b. Enter the MCC and MNC values.

> **Note**
>
> The **New** button remains unavailable until valid values are entered in both fields.

   c. Select **New** to accept the entered values and open a new row.

4. Once you have finished configuring the **SP Identification** tab, select **OK** to save the configuration.

Related Topics

     Configure Hotspot on page 189

     Hotspot Identification on page 190

     Network Characteristics on page 194

     Online Signup on page 196

NEW! *Network Characteristics*

The hotspot Network Characteristics tab displays network parameters for the hotspot.

To configure Network Characteristics for the hotspot:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 189.

2. Select the **Network Characteristics** tab.

Figure 40: Configuring Network Characteristics

3. Configure the following parameters:

IP Address Type Availability. The mobile device uses the IP Address Type Availability information to make network selection decisions. Select the level of restriction for each network type.

IPV4 valid values are:

- Not Available
- Public
- Port Restricted
- Single NAT
- Double NAT
- Port Restricted Single NAT
- Port Restricted Double NAT
- Unknown

IPV6 valid values are:

- Not Available
- Available
- Unknown

WLAN Metrics. Enter the values for maximum Uplink and Downlink speed and load parameters for the WLAN service.

The mobile device uses information from the WAN Metrics configured here to make network selection decisions. The mobile device can determine if necessary throughput is available from the hotspot before connecting. If the mobile device receives indication that the basic service set (BSS) is at capacity, the device will not associate with that AP.

Connection Capability. The mobile device uses connection capability information to make network selection decisions by determining which services are blocked or supported at the hotspot. Configure up to 16 ports.

- To add a protocol, select **New**. Select the protocol, the port number, and the status associated with the protocol. Valid status values include: Closed, Open, or Unknown.

> **Note**
> Make an effort to configure all ports and do not rely on the Unknown value.

4. Once you have finished configuring the **Network Characteristics** tab, select **OK** to save the configuration.

Related Topics

NEW! Online Signup

The hotspot **Online Signup** tab displays hotspot properties for Online Signup (OSU) users. Online Signup allows users who are not part of the provider network to manually connect to the hotspot. It also allows for added security for users who want to connect anonymously. To configure Online Signup, you must configure a separate WLAN for OSU with Open Authentication or WPA2-Enterprise (802.1x/EAP). Encryption is specific to the service provider. Credentials in the mobile device SIM Card authenticate the user.

To configure the OSU WLAN that you will specify on the **Online Signup** tab:

1. Go to **Configure** > **Network** > **WLAN Settings**.
2. From the Hotspot field, select **OSU**.
3. From the Auth Type field, select **Open** or **WPA2-Enterprise (802.1x/EAP)**.

> **Note**
> You will specify this OSU WLAN in the Online Signup configuration.

To configure Online Signup for the hotspot:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 189.
2. Select the **Online Signup** tab.

Figure 41: Configuring Online Signup

3. Configure the following parameters:

   Network Authentication Type. Possible values for network authentication are:
   - Acceptance of terms and conditions. Redirection is accomplished after user accepts Terms and Conditions.
   - Http/Https redirection. Redirect Http or Https automatically. Provide the Redirection URL.
   - Online enrollment supported. Authentication supports online enrollment. Service Provider configuration pane displays.
   - DNS redirection. DNS redirection serves a web page other than what the end user had requested.

   OSU WLAN. This is the address of the Online Signup WLAN. Create this WLAN separately. The Auth Type for the OSU WLAN can be either Open or WPA2 Enterprise. Encrypted Authentication is specific to the Service Provider. Network Authentication is available in the SIM Card of the mobile device.

   Server Provider Setting. This is service provider configuration settings.
   - To add a provider to the list, select **New** and configure the provider settings. For more information, see Configuring the OSU Service Provider on page 198.
   - To remove a provider from the list, select the list row, then select 🗑.

- To edit provider information, select the list row, then select ✏. For more information, see Configuring the OSU Service Provider on page 198.

4. Select **OK** to save the Online Signup configuration.

Related Topics

Configuring the OSU Service Provider on page 198

Configure Hotspot on page 189

NEW! **Configuring the OSU Service Provider**

Hotspot configuration supports Online Signup. This task outlines how to create a list of service providers that support Online Signup.

Take the following steps to configure an Online Signup service provider:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 189.
2. From the WLAN Services Hotspot tab, select the **Online Signup** tab.

3. In the Service Provider Setting pane, select **New**.
   The **OSU SP Configuration** dialog appears.

OSU SP Configuration

Server URI

Methods   CHANGE ORDER

   ☐   OMA

   ☐   SOAP

Icon   CHANGE   REMOVE

Anonymous Name

Language 1

Language ▼

Friendly Name

Service Description

Language 2

Language   -   ▼

Friendly Name

Service Description

Figure 42: Configuring the OSU Service Provider

4. Configure the following parameters:
   Server URI

The OSU server URI.

Methods

OSU Method is the preferred list of encoding methods that the OSU server supports in order of priority. Select the connection method used by the provider. Select **Change Order** to reorder the method priority.

Icon

Add an icon that is associated with Online Signup:

- To add or change the icon, select **Change**. Then, navigate to a .png file.
- To remove the icon, select **Remove**.

Anonymous Name

Configure a name that anonymous users can use to access the network.

Language

Configure the Language, Friendly Name, and Service Description for the Online Signup user interface.

5. Select **OK** to save the OSU SP configuration.

Related Topics

Captive Portal Settings

Go to **Networks** > **WLANS** to enable captive portal. Select the portal type: Internal, External, or CWA (Centralized Web Authentication). The configuration settings depend on the portal type.

> **Note**
> By default, when captive portal is enabled, HTTP, DNS, and DHCP access is provided to Extreme Campus Controller for redirection.

Related Topics

Internal Captive Portal Settings

An internal captive portal resides on Extreme Campus Controller. Configure the following parameters for an internal captive portal.

Table 59: 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. Select **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 60: 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 60: External Captive Portal Settings (continued)

Field	Description
Identity	Determines the name common to both the Extreme Campus Controller and the external Web server if you want to encrypt the information passed between the Extreme Campus Controller and the external Web server. Required for signing the redirected URL. If you do not configure the Identity, the redirector on the AP drops the traffic.
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

Centralized Web Authentication

Typically, when an external captive portal is employed, a web server hosts a single site that allows users to authenticate to the network. Centralized Web Authentication (CWA) offers the ability to serve a web page based on a set of conditions that are defined on the RADIUS server. The user is redirected to the appropriate web page after successful authentication using the 802.1x protocol.

With a CWA captive portal, the URL for the captive portal is provided dynamically through RADIUS attributes. The redirection can occur either at the AP (for bridged@AP topologies) or at Extreme Campus Controller (for bridged@AC topologies). Examples of conditions that determine the destination web page include: the expiration date for a user password, or the due date of a bill that must be paid before a user can gain access to the network.

CWA supports an ExtremeControl captive portal server and a Cisco® ISE captive portal server. The configuration procedure for captive portal on Extreme Campus Controller is the same regardless of the captive portal server. CWA is supported on both Bridged@AC and Bridged@AP topologies.

From Extreme Campus Controller, you must configure the following:

• Configure a AAA Policy, defining the RADIUS server, then specify that AAA Policy on the CWA captive portal network configuration.
• Configure a policy role that includes a redirect rule. The redirect rule must use the TCP protocol and redirect the client based on the domain name or IP address that is specified in the URL message that is sent from the RADIUS server.

For information on the captive portal server configuration, see the Extreme Campus Controller Deployment Guide.

> **Note**
>
> AP39xx access points do not support Centralized Web Authentication (CWA) captive portal.

Related Topics

CWA Network Settings

To configure a Centralized Web Authentication (CWA) captive portal:

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

Figure 43: CWA Network on Extreme Campus Controller

2. Configure the following settings:

Table 61: Centralized Web Authentication Network Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Maximum 32 characters. Upper and lowercase allowed. Example: PermanentStaff
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.
Auth Type	The Authorization Type for a CWA captive portal must be **WPA2 Enterprise (802.1x EAP)**
Enable Captive Portal	Select this option to configure a captive portal network.

MAC-Based Authentication	(Optional) Select this option to enable MBA. When selected, multi-factor authentication is enabled. The following parameter displays when MAC-based Authentication is enabled:
	• **MBA Timeout Role**. Select the role that will be assigned to a wireless client during MAC-based authentication (MBA) if the RADIUS server access request times out. If no MBA Timeout Role is selected, then a RADIUS server timeout is treated like an Access-Reject, which prevents the client from accessing the network. Other options:
	  ◦ ⊙ — create a new role
	  ◦ ◪ — edit role
	  ◦ ☐ — delete role

Captive Portal Type	**CWA**
AAA Policy	Specify the AAA Policy associated with the captive portal. Define the RADIUS server used for authentication in the AAA Policy. This is the IP address of the captive portal. See Figure 44 on page 205.
Default Auth Role	Specify the default authorization role that is configured on Extreme Campus Controller.
Default VLAN	Specify the default VLAN that is configured on Extreme Campus Controller.

Figure 44: AAA Policy for CWA — RADIUS Server definition

Related Topics

Configure AAA Policy on page 243

CWA Policy Redirection Role on page 205

Add Policy Roles on page 214

Configuring VLANS on page 224

CWA Policy Redirection Role

To configure a policy role with at least one redirection rule:

1. Go to **Configure** > **Policy** > **Role** > **Add**.
2. Create a new role.
3. Select **Layer 3/Layer4** and configure the parameters for a redirect rule that works with CWA captive portal. See Table 62 on page 207.

Figure 45: Example Redirection Role on Extreme Campus Controller that includes six L3/L4 rules

Figure 46: Redirect-80 rule redirects HTTP traffic from Port 80

Table 62: Rule Configuration for Layer3/Layer4 Redirection Rules

Field	Description
Name	Provide a name for the rule. Example: **Redirect-80** that redirects traffic on HTTP port 80.
Action	**Redirect**
Protocol	**TCP**
IP/Subnet	**User-Defined**. Then specify the IP address of the captive portal.
Port	Include at least one rule for HTTP port 80 or HTTPS port 443

Related Topics

ExtremeGuest Captive Portal Settings

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

Table 63: 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 Extreme Campus Controller unregistered access policy must allow access to the third-party site (either allow all SSL or

make allowances for third-party servers). The Portal Configuration must have the specific site registration enabled and include the Application ID and Secret for the third-party site.

Third-party registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

Create a unique application to the third-party software. Refer to the following developer sites:

- Facebook Developers page at https://developers.facebook.com/apps/
- Google Developers page at https://console.developers.google.com/projectselector/apis/library
- Microsoft Developers page at https://apps.dev.microsoft.com/#/appList.
- Yahoo Developers page at https://developer.yahoo.com/
- Salesforce Developers page at https://developer.salesforce.com/

The Application ID and Application Secret assigned during the creation of the third-party application must be provided in the Portal Configuration page.

> **Note**
> With an Availability Pair, when configuring authentication in the portal, specify the URI (*Uniform Resource Identifier*) for both the Primary and Secondary appliance.

Related Topics

Adding Walled Garden Rules

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 64: FQDN Rules Required for Social Logins

Application Site	Rule Parameters
Facebook	• Allow FQDN to facebook.com, port HTTPS • Allow FQDN to fbcdn.net, port HTTPS
Google	• Allow FQDN to accounts.google.com, port HTTPS
Microsoft	• Allow FQDN to login.live.com, port HTTPS • Allow FQDN to gfx.ms, port HTTPS • Allow FQDN to akadns6.net, port HTTPS
Salesforce	• Allow FQDN to login.salesforce.com • Allow FQDN to sfdcstatic.com
Yahoo	• Allow FQDN to login.yahoo.com, port HTTPS • Allow FQDN to yimg.com, port HTTPS

Related Topics

Walled Garden Rules on page 207

Configuring L2 Rules on page 216

Configuring L3, L4 Rules on page 217

Configuring L7 Application Rules on page 219

Captive Portal Redirect Port List

Configure a port on the Extreme Campus Controller interface to which the client is redirected after the ECP response. If ECP support is configured for HTTP then the port is typically **80**, otherwise it is typically **443**. It is possible to configure a different port. The hw_port attribute appears in the redirection response from Extreme Campus Controller.

1. Go to **Configure** > **Networks** > **WLANS**.
2. Select **Enable Captive Portal**.
3. Select **CP Redirect Port List**.
4. Select ⊚ to add a port to the list.
5. To delete a port, select the port, and then select 🗑.

Advanced Network Settings

To configure advanced network settings:

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

   Auto Provision OWE Network

   Enable this option to generate an Opportunistic Wireless Encryption (OWE) network automatically when the network authentication is set to Open. OWE offers security to open networks, ensuring that traffic between an AP and a client is encrypted. Other clients can sniff and record traffic, but cannot decrypt it.

Agile Multiband

Enables wireless devices to better respond to changing wireless network conditions. Improved resource utilization helps balance wireless network load, increase capacity, and provide end users the best possible wireless experience.

This feature is enabled by default. It is supported on ExtremeWireless access points AP3xx, AP4xx, and AP5xx.

RADIUS Accounting

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

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 Extreme Campus Controller.

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

NEW! *Configuring DSCP Classification*

A Differentiated Services Code Point (DSCP) is a packet header value that indicates Quality of Service (QoS) priority level for traffic delivery. All 64 DSCP code-points are supported.

To define a class of service for each DSCP code:

1. Go to **Configure** > **Networks** > **WLAN Services**.
2. Select a network or select **Add**.
3. Select **Advanced**.
4. Scroll to the bottom of the **Advanced Settings** page and select **QoS/DSCP**
5. Select a Service Class value for each DSCP code.

   Valid priority values in descending order:
   - Network Control (7)
   - Premium (Voice) (6)
   - Platinum (5)
   - Gold (4)
   - Silver (3)
   - Bronze (2)
   - Best Effort (1)
   - Background (0)

Related Topics

Advanced Network Settings on page 209

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

WLAN Service Settings on page 180
Mesh Point Network Settings on page 188
Networks List on page 76

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.

Extreme Campus Controller is shipped with a default policy configuration that includes the following default roles:

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

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

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

Related Topics

Add Policy Roles

Define policy roles to provide unique treatment of packet types when a single role is applied.

> **Note**
>
> Associate each role with a configuration Profile of a device group for each AP in the group to make use of the policy role.

1. Go to **Configure** > **Policy** > **Roles** > **Add**.
2. Configure the parameters for the role. For more information, see Policy Role Settings on page 214.
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 Extreme Campus Controller. Policy rules are applied from top to bottom.

4. To add new rules, select **New**.

   > **Note**
   >
   > ExtremeWireless Wi-Fi 6 access points support rule sets that contain up to 256 rules. AP39xx series access points support rule sets with no more than 64 rules.

5. To edit a rule, click on the rule to open the rule parameters. Configure the rule parameters and select **Save**.

   > **Note**
   >
   > If you create a Deny All rule for any subnet as the top rule, the policy will drop all traffic.

Related Topics

Policy Role Settings

Table 65: 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.

Table 65: Role Parameter Settings (continued)

Field	Description
Default Action	Determines the access control default action. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. However, if you require user-specific filter definitions, then the filter ID configuration identifies the specific role that is applied to the user. Valid values are: • Allow. Allow packets using the specified VLAN option. Specify either the Default Network VLAN or a configured VLAN. • Deny. Deny packets that do not match a filter rule or deny packets when a filter rule does not exist. When a packet *does* match the filter rule action Allow, allow packet using the specified VLAN option. Specify either the Default Network VLAN or a configured VLAN.
VLAN ID	Policy roles default to the VLAN specified during network configuration. You can specify a unique VLAN here. Click ⊕ to add a new VLAN option.
Associated Profile	Indicates profiles that this role is associated with. Click ✎ to modify profile association. **Note:** Associate a role with a configuration Profile. The configuration Profile is associated with the device group. Each AP in the device group makes use of the policy role.
Rules	Policy rules are organized by Open Systems Interconnection (OSI) layer classification. Select the drop-down arrow to display rules that pertain to each OSI layer.

Related Topics

Policy Rules for OSI L2 to L4

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

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.

Extreme Campus Controller installs application policies with rules on the supported APs where enforcement occurs.

> **Note**
> Application policies are supported by Extreme Campus Controller-enabled APs only, not switches.

Rules

Application policies consist of rules with matching criteria, coupled with one or more actions to take when a packet matches the rule's criteria. The matching criteria for an application is usually just the name of the application. The Extreme Campus Controller user interface lets you first select a category of applications, resulting in a subset of applications to choose from. Additionally, you can create a single rule that applies to all traffic in the application category by selecting a category and then selecting 'Wild Card' as the specific application.

Custom application rules are rules that you create to recognize (match) applications that are not in the pre-defined set of application matches provided by Extreme Campus Controller. You create a custom application rule by defining a regular expression to match against host names. The rule's match criteria will be available as a match criteria for policy rules that you create in the future.

Actions and Limitations

When the Action filter for the application rule is set to Deny, the first few packets of a flow must be allowed to pass through so that the deep-packet inspection (DPI) engine can examine the contents and classify the packets. 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

Adding Custom Apps to the Application List on page 220

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 221

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 66: 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 on page 221
Configuring ToS/DSCP on page 222

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 the controller, VxLAN, 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. Extreme Campus Controller preconfigures switches with a single untagged VLAN that is used for managing access points and the switches themselves.

Another common option is to place all traffic on a single untagged VLAN. This is a simpler option to use when a network's applications do not benefit from VLAN deployment.

Extreme Campus Controller fully supports mixing tagged and untagged traffic. An AP wired interface can be an untagged member of one VLAN and a tagged member of several other VLANs simultaneously.

With switches, all administrator-created VLANs in Extreme Campus Controller are classified as tagged VLANs. When a tagged VLAN is assigned to a port, the port is configured to expect all traffic received from the VLAN or sent to the VLAN to be tagged. You can override the tagging on a per-port basis for the ports types Host and Other.

Associate a topology to a specific device group. This allows you to define a topology that is common to a set of devices and specify a specific attached VLAN.Topologies referenced by attached networks or roles are automatically added to the Profile VLANS list. You can also add topologies manually to the list. When creating a new topology, select the Profiles to associate with the new topology.

Related Topics

Configuring VLANS

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 67: VLAN Configuration Settings

Field	Description
Name	Provide a unique name for the VLAN.
Mode	**Bridged@AC** — The Extreme Campus Controller bridges traffic for the station through its interfaces, rather than routing the traffic. For B@AC, topology the station's "point of presence" on the wired network is the data plane port assigned to the topology. **Bridged@AP** — Assigned to APs, the AP bridges traffic between its wired and wireless interfaces without involving the Extreme Campus Controller. 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 Extreme Campus Controller anywhere a B@AP topology can be configured. **VxLAN** — VxLAN is a network virtualization technology that leverages existing Layer 3 infrastructures to create tenant overlay networks. VxLAN addresses the requirements of a multi-tenant data center network infrastructure by: • Increasing virtual network scalability to 16 million instances. This allows for tenant VLAN (Virtual LAN) isolation whereby multiple tenants can manage their own VLAN/VMAN and MAC address spaces. • Adding an encapsulation that effectively hides VM MAC addresses from the physical network that results in physical networking devices to have smaller MAC and IP table sizes. • Allowing for Layer 2 adjacency across IP networks by which DC network operators protect their investment in their current infrastructure. Additionally operators can distribute traffic loads across links efficiently using Layer 3 ECMP (Equal-Cost Multi-Path routing).
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.
VNI	For **VxLAN**. VxLAN Network Identifier. The VNI is a 24-bit identifier. It can be used in more than one VxLAN topology.

Table 67: VLAN Configuration Settings (continued)

Field	Description
Remote VTEP	For **VxLAN**. The IP address of the tunnel End-Point is referred to as a VxLAN Tunnel Endpoint (or VTEP). The VTEP is the IP address of the network switch. Network switches that act as a VTEP are referred to as VxLAN gateways. There can only be one VTEP per VxLAN topology.
I-SID	For **Fabric Attach**. A unique VLAN identifier and a unique I-SID (service identifier). The I-SID range is (0-15999999). Use **I-SID = 0** to support Fabric Attach Standalone Proxy mode on Extreme Networks Ethernet Routing Switches. Standalone Proxy mode indicates that the network does not include a Fabric Attach Server switch (and therefore does not include a Shortest Path Bridging Fabric Core).
Tagged Traffic	If you have more than one VLAN on a port, enable tagging to identify to which VLAN the traffic belongs. Ensure that the tagged vs. untagged state is consistent with the switch port configuration. Fabric Attach topologies are always tagged.
Port	The port for network traffic bridged at controller (for example, physical ports: Port0, Port1, Port3, Port4). LAG ports are supported on physical appliances only (LAG1, LAG2).
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 Extreme Campus Controller via this IP address.
FQDN	Fully-Qualified Domain Name
CIDR	CIDR field is used along with IP address field to find the IP address range.
DHCP	Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses. Valid values are: • Local Server. Indicates that the Extreme Campus Controller is used for managing IP addresses. • Use Relay. Indicates that the Extreme Campus Controller forwards DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the Extreme Campus Controller and allows the enterprise to manage IP address allocation to a site from its existing infrastructure.
Enable Device Registration	Indicates that the wireless AP or switch can use this port for discovery and registration.

Table 67: VLAN Configuration Settings (continued)

Field	Description
Mgmt Traffic	Indicates that this port will be used to manage traffic. Enable **Mgmt Traffic** to access the Extreme Campus Controller user interface through this port.
Associated Profiles	Select ▧ to display a list of configured Profiles. You can associate a VLAN to a specific set of devices through the assigned configuration Profile for the device group.

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

5. Select **Save**.

Related Topics

VLAN Advanced Setting

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. Extreme Campus Controlleroffers a predefined set of multicast rules. Select a preset multicast rule or define a new rule.

Related Topics

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.

NEW! **Local DHCP Management Settings**

Configure the following Local DHCP settings:

Domain Name

The name of the domain that is allocated for the IP address range.

Lease (Seconds)

The DHCP Lease represents the time period between when a device obtains the IP address and the time the IP address expires. When the **Lease** expires, the device releases the IP address and Extreme Campus Controller issues a new one. Default Lease is 36000 seconds, Default Max Value is 2592000 seconds. Devices can request a lease value.

DNS Servers

Primary IP address for the DNS (Domain Name Server).

WINS Servers

IP address of the WINS (Windows Internet Name Service) server.

Gateway

Gateway IP address.

Address Range

IP address range. Value is prompted by the subnet IP address that you configured.

Exclusions

(Available from the VLAN configuration) A range or single IP address that is excluded from the greater Address Range. Save your VLAN configuration before selecting **Exclusions** to configure IP address exclusions.

Related Topics

NEW! Configure IP Address Exclusions

Exclude specific IP addresses or a range of IP addresses when configuring the IP Address Range for the Local DHCP server.

> **Note**
> Save your VLAN ID configuration before configuring IP Address Range Exclusions for a Local DHCP.

1. From the **Local DHCP Settings** dialog, select **Exclusions**.
2. Configure an IP Address Range or a Single IP Address that will be excluded from the larger IP Address Range configured under **Local DHCP Settings**.
3. Add an optional comment indicating why these addresses are excluded.
4. To add a new comment, select **New**.
5. To save the excluded IP addresses, select **Save**.
6. After you save, you can edit or delete the saved exclusions:

   - To edit the saved exclusions, select ✏.
   - To delete the saved exclusions, select 🗑.

Related Topics

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 Extreme Campus Controller anywhere a B@AP topology can be configured.

> **Note**
> When Fabric Attach is configured, LLDP (Link Layer Discovery Protocol) is automatically enabled on all APs associated with the topology. The setting cannot be disabled by users.

The switch requires that the VLAN/I-SID mapping is unique per port per switch, therefore only one AP per switch port is allowed.

ExtremeWireless APs connected to a Fabric-enabled switch automatically use the default management VLAN that is configured on the switch. Moving an AP from a Fabric-enabled switch to a non Fabric-enabled switch requires a factory default reset to connect to the new management VLAN.

> **Note**
> In a mobility scenario that includes a local and foreign Extreme Campus Controller, make sure the Fabric Attach topology configuration is the same on each Extreme Campus Controller, ensuring that an AP that moves between appliances has the same set of topologies.
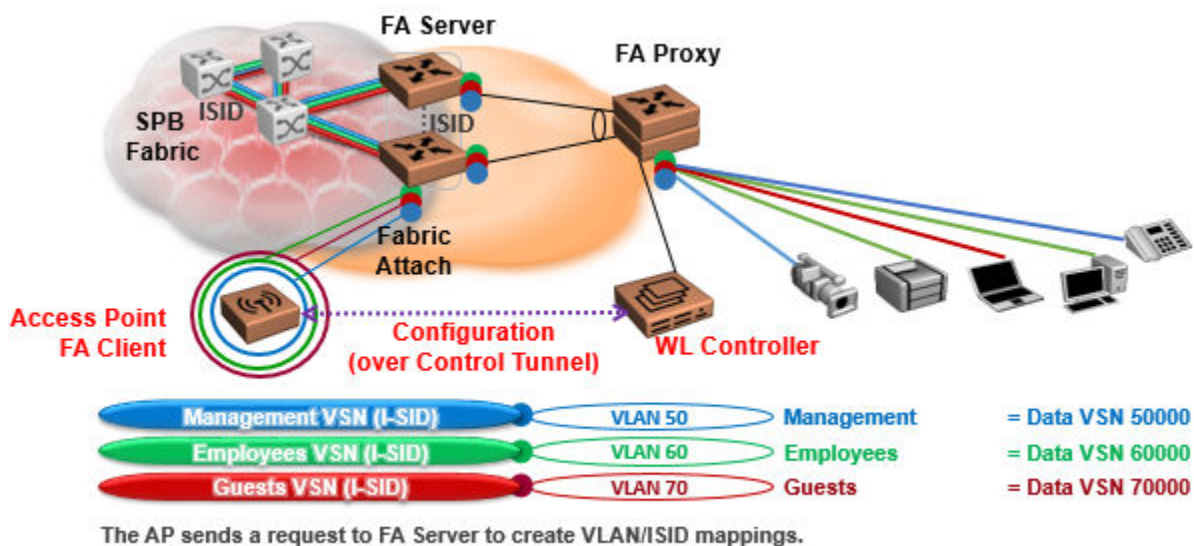

Figure 47: Fabric Attach for FA Clients — Automated Network Services

VxLAN Topology

Extreme Campus Controller leverage VxLAN capabilities of ExtremeXOS switches to establish different head-ends for tunneling traffic in an enterprise. Support includes:

- Tunnel in VxLAN from AP directly to a target switch
- Bypass Extreme Campus Controller
- Abstracts interconnections.

VxLAN is a Layer 2 overlay scheme over a Layer 3 network. Overlays are called VxLAN segments and only a VM and a physical machine (tenant) within the same segment have Layer 2 connectivity. VxLAN segments are uniquely identified using an identifier called the VxLAN Network Identifier (VNI). The VNI is a 24-bit identifier; therefore, an administrative domain can support up to 16 million overlay networks.

Because the scope of the MAC, originated by tenants, is restricted by the VNI, overlapping MAC addresses across segments can be supported without traffic leaking between tenant segments. When a tenant frame traverses a VxLAN overlay network, it is encapsulated by a VxLAN header that contains the VNI. This frame is further encapsulated in a UDP header and L2/L3 headers.

VxLAN can add up to a 50-byte header to the tenant VM frame. For VxLAN to work correctly, this requires that the IP MTU be set to at least 1550 bytes on the network-side interfaces. IP MTU of 1550 should also be set on all transit nodes which carry VxLAN traffic. The point at which a tenant frame is encapsulated (or decapsulated) is referred to as a VxLAN Tunnel Endpoint (or VTEP). VTEPs are typically located on hypervisors but may also be located on physical network switches. Network switches that act as a VTEP are referred to as VxLAN gateways.

The role to encapsulate/decapsulate a frame is performed by a VxLAN Tunnel Endpoint (VTEP), also referred to as a VxLAN gateway. A VxLAN gateway can be a Layer 2 gateway or Layer 3 gateway depending on its capacity. A Layer 2 gateway acts as a bridge connecting VxLAN segments to VLAN segments. A Layer 3 gateway performs much like a Layer 2 gateway, but it is also capable of routing traffic between tenant VLANs.
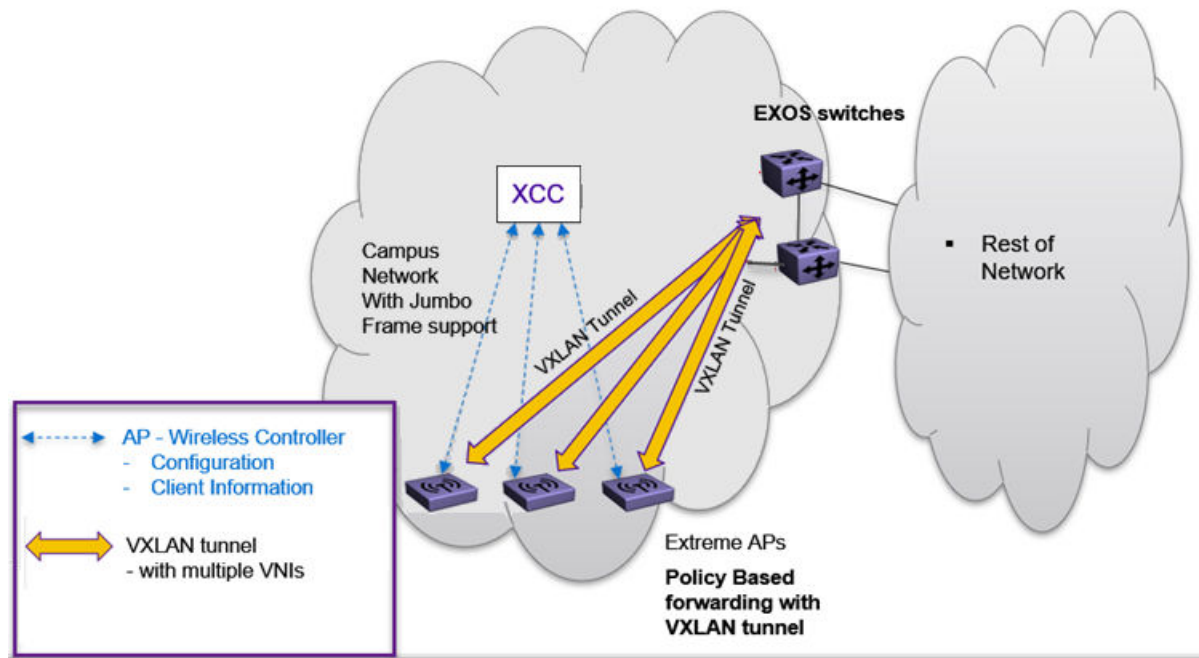

Figure 48: VxLAN Topology

Related Topics

Configuring a VxLAN in Extreme Campus Controller

A VxLAN topology in Extreme Campus Controller can be supported in the following configurations:
* A default VLAN for policy roles
* Contain to VLAN action for policy rules
* A default VLAN for network configuration

VxLAN is supported on a Centralized network with Jumbo-Frame support. You are not required to explicitly enable Jumbo Support on the AP. The network path that the tunnel will traverse, from AP to VTEP switch must be provisioned for Jumbo Frame support for at least 1550 byte packets. The AP does not require a special setting in regards to handling larger frames towards the clients. The AP and

switches must be at least one hop away, and all devices between the AP and the ExtremeXOS switch must allow Jumbo-Frame of IP 1550 bytes.

The following ExtremeXOS switches and APs support a VxLAN topology:

- **ExtremeXOS Switches:**
  - X465
  - X590
  - X690
  - X695
  - X870
  - X670-G2
- **ExtremeWireless access points:** AP3xx, AP4xx, and AP5xx with firmware version WiNG 7.4.0 or later.

When configuring a VxLAN topology, configure only one VNI and one VTEP (switch IP address). If you have a VNI that associates with more than one VTEP (switch IP address), you must configure a separate VxLAN topology. You can use the same VNI, but associate it to a different VTEP (switch IP address).

Due to a hardware limitation of 512 access points per switch, configure more than one VxLAN topology in a deployment that manages more than 512 access points. Each topology configuration can use the same VNI with a different VTEP.

> **Note**
> The VLAN ID in the VxLAN topology is shared within the Bridge@AP VLAN ID pool. The VLAN ID cannot be duplicated among the Bridge@AP, Fabric Attach, and VxLAN topologies for the same AP. Extreme Campus Controller does not allow a duplicate VLAN ID per site.

To configure a VxLAN topology in Extreme Campus Controller:

- Go to **Configure** > **Policy** > **VLANs**.
- Select **Add** and configure the VLAN parameters.

Related Topics

Configuring VLANS on page 224
VxLAN ExtremeXOS Considerations on page 231

VxLAN ExtremeXOS Considerations

Consider the following items before configuring a VxLAN topology with ExtremeXOS switches:

- The physical interface that handles the ExtremeXOS local endpoint IP address must be different than the attached physical port for the Tenant VLAN for VxLAN VNI. You must have at least two trunk ports to separate local endpoint traffic and tenant VLAN traffic.

  Example:
  ```
  configure vlan VLAN_3000 add ports 48 tagged
  configure vlan VLAN_3000 ipaddress 10.47.1.104 255.255.254.0
  configure virtual-network local-endpoint ipaddress 10.47.1.104 vr "VR-Default"

  configure vlan VLAN_3105 add ports 47 tagged
  configure virtual-network "IDAP" vxlan vni 8192
  configure virtual-network "IDAP" add vlan VLAN_3105
  configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.100 vr VR-
  Default
  ```

```
configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.108 vr VR-
Default
configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.109 vr VR-
Default
```

- A remote endpoint (AP) must be at least one hop away from the ExtremeXOS local endpoint.

  The configuration must include at least one gateway router between the AP and the switch. The gateway must enable IP MTU (Maximum Transmission Units) of 1550 bytes.

  Example:

```
configure vlan VLAN_3000 add ports 48 tagged
configure vlan VLAN_3000 ipaddress 10.47.1.104 255.255.254.0
configure virtual-network local-endpoint ipaddress 10.47.1.104 vr "VR-Default"

configure vlan VLAN_3105 add ports 47 tagged
configure virtual-network "IDAP" vxlan vni 8192
configure virtual-network "IDAP" add vlan VLAN_3105
configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.100 vr VR-
Default
configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.108 vr VR-
Default
configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.109 vr VR-
Default
```

VLAN Groups

A VLAN group can be associated with a single wireless network. In a large venue, a VLAN group can support many wireless clients on a single WLAN. The wireless client can associate with any VLAN in the group. The association is determined by a MAC address hashing algorithm.

> **Note**
> Bridged@AC topologies using AP39xx access points are supported.

To access VLAN Groups, go to **Configure** > **Policy** > **VLAN Groups**.

- Select a group to view or edit.
- Select **Add** to add a new group.

Consider the following with VLAN Groups:

- Bridged@AP and Fabric Attach topologies are not supported.
- In the case of a VLAN ID conflict, the member VLAN ID takes precedence over the group VLAN ID.

Related Topics

VLAN Group Settings

To create a VLAN Group:

1. Go to **Configure** > **Policy** > **VLAN Groups**.
2. Click **Add**.
3. Configure the following parameters:

   Name

   Group name.

Mode

- **Bridged@AC** topologies using AP39xx access points are supported.

> **Note**
> You cannot modify the group mode after the group is created.

VLAN ID

ID for the VLAN Group

VLANs

List of configured VLANs that can be added to the group. Select a VLAN from the list and click the plus sign to add the VLAN to the group.

4. Click **Save**.

Related Topics

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**.

Automatic Adoption

The adoption feature simplifies the deployment of a large number of access points and switches. A set of rules defines the device group assignment for new devices, when they register for the first time. Without adoption rules defined, you must manually select each device for inclusion in a device group.

> **Note**
> Without adoption rules, when a device group configuration matches the device license domain and model number, Extreme Campus Controller prompts you to add the devices, but you must manually select each device for inclusion in the device group.

Adoption rules support the following:

- Automatic adoption of access points and switches based on matching criteria
- Site and device group assignment based on matching criteria
- Device adoption denial based on matching criteria
- Device redirection to a different Extreme Campus Controller

- Site and a device group assignment based on a partial match of the FQDN or DNS suffix
- Event Logging of the device adoption process

Related Topics

Adoption Rules

To avoid a manual process, create adoption rules before you register devices. Adoption rules organize access points and switches based on preset conditions or rules.

When you are ready to register one or more devices:

1. Create the logical device groups for the access points within a site.
2. Configure the adoption rules that populate the groups.
3. Register the devices.

   The APs are organized into the logical sites and device groups automatically, based on the adoption rule definitions. Switches are associated with the logical sites, but not assigned to device groups. Rules are evaluated from the top down. Use the up and down arrows to put adoption rules in a specific order. If the device does not match the criteria of the first adoption rule, then the next rule is evaluated.

   Note

   For AP adoption only — In addition to matching rule criteria, the site and device group configuration must match the AP for the adoption rule to take effect. The AP license domain must match the site Country, and the AP model number must match the site Type and device group Profile configuration.

Related Topics

Adding or Editing Adoption Rules

Adoption rules filter on one or more of the following network attributes:

- Model — Matching criteria is a sub-string. For example, if filter criteria is FCC, all APs with FCC in the model number will match.
- Host Name — Matching criteria is a sub-string.

- IP Address / CIDR — Enter a single IP address for each rule. The range for CIDR is 0 to 32. If the CIDR is 0, the IP address will not be used as a matching criteria.
- Serial Number — Matching criteria must be an exact string. Enter a single serial number for each rule.

> **Note**
> To successfully match an adoption rule, all specified parameters must match.

To add or edit an adoption rule:

1. Go to **Configure** > **Adoption**.
2. To add a new rule, select **Add**.
3. To edit an existing rule, select an adoption rule in the list, and then select ✏.

Related Topics

Configure AP Adoption Rule

Specify a site and device group when creating an AP adoption rule.

1. Go to **Configure** > **Adoption** > **Add**.

   The **New Rule** dialog displays.
2. To create a rule for access points, select **AP**.
3. For **Action**, select one of the following values:
   - Allow
   - Deny
   - Redirect
4. Select the site associated with the adoption rule.

   The site holds the device group. The device group includes the APs that meet the filter criteria.

   Pattern-Based refers to adopting access points based on their domain. For more information, see Pattern-Based Matching on page 236.
5. Select a device group that will contain the APs that meet the filter criteria.
6. Select a filter parameter, and then select ⊕.

> **Note**
> Each filter value can only be applied once to a single rule.

Related Topics

Configure Switch Adoption Rule

Specify a site when creating a switch adoption rule. The device group does not apply to switches.

1. Go to **Configure** > **Adoption** > **Add**.
   The **New Rule** dialog displays.
2. To create a rule for switches, select **Switch**.
3. For **Action**, select one of the following values:
   - Allow
   - Deny
   - Redirect
4. Select a site.
5. Select a filter parameter, and then select ⊕.

Related Topics

Adoption Rule Filters on page 239

Configure Device Redirection on page 239

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 Extreme Campus Controller. The assignment is based on the matching criteria for the $FQDN or $DNS-SUFFIX variables.

> **Note**
> Before you define a Pattern-Based adoption rule, you must create a site and device group using a name that will match the name defined by the variables. Coordinate your variable definitions with the names of your existing sites and device groups. Then, create the adoption rules configuring variables with specific index definitions that will result in a match to the site name or device group name that you created.

An adoption rule is comprised of a filter definition and a site and device group definition. First, the rule matches the device attributes to the defined filter criteria. Then the rule assigns those devices to a site or device group based on the $FQDN or $DNS-SUFFIX variable values that match existing sites and device groups.

The FQDN and DNS suffix must follow a consistent format for Pattern-Based matching to be successful. One Pattern-Based rule definition can assign devices to any number of configured sites and device groups based on successful variable matches. When the defined pattern *does not* match an existing site or device group, an error is logged and Extreme Campus Controller continues evaluating the next adoption rule.

Examples: Variable Definitions

`$FQDN[x:y]`

Uses the sub-string of the Fully-Qualified Domain Name reported by the device, from character at position x to character at position y. The first character is position 1 (not 0). The value 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 — Specify a device group pattern "AP510-$FQDN[6:8]". The AP reports a FQDN as "ap510RDU.cath.extremenetworks.com". Based on the variable definition index [6:8], the AP is assigned to the device group named AP510-RDU. For Pattern-Based matching to work, in this example, you must have a device group previously configured that is named AP510-RDU. If that device group does not exist, an error is logged and the rules engine continues evaluating adoption rules.

`$DNS-SUFFIX[x:y]`

Uses the sub-string of the Domain Name Server suffix reported by the device, from character at position x to character at position y. The first character is position 1 (not 0). The value 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 existing site is named Site_RDU. My variable is defined as Site_$DNS-SUFFIX[1:3]. Variable index [1:3] results in a site named Site_RDU. Characters 1 to 3 in the DNS suffix results in RDU.

If you are consistent with the naming convention for sites, device groups, and FQDNs, you will be able to use one rule to assign any AP regardless of the specific AP model or domain name.

Related Topics

Configure Adoption Based on FQDN or DNS Suffix

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 236.

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 239
Pattern-Based Matching on page 236

Configure Device Redirection

You can configure an adoption rule that redirects devices to another appliance when matching criteria are met.

> **Note**
> AP39xx access points do not support adoption rule redirection where the redirected destination is defined as an FQDN. AP39xx only supports a redirected destination that is defined as an IPv4 address.

1. Go to **Configure** > **Adoption** > **Add**.

   The **New Rule** dialog displays.

2. Select the device type:

   - To create a rule for access point adoption, select **AP**.

   - To create a rule for switch adoption, select **Switch**.

3. From the **Action** field, select **Redirect**.

   The **IP Address** field is displayed.

4. Provide the IP address of the destination Extreme Campus Controller.

5. Select a filter parameter, and then select ⊕.

> **Note**
> Devices that match filter criteria on a redirect action do not connect to Extreme Campus Controller initially. They are redirected to another Extreme Campus Controller. If the destination Extreme Campus Controller contains adoption rules with filter criteria that match the redirected devices, the devices are adopted by the destination Extreme Campus Controller. You must configure adoption rules on the second appliance as a separate action from the redirection. Adoption to the second appliance is not included in the redirect action.

Related Topics

Adoption Rule Filters on page 239

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 Extreme Campus Controller.

IP Address/CIDR

Filter the APs or switches by IP address, adopting APs into the specified device group based on their IP address. CIDR field is used along with IP address field to find the IP address range.

For switch adoption rules, specify the management IP address.

Host Name

Filter the APs by host name, adopting APs into the specified device group based on their host name. This field matches on sub strings.

For switch adoption rules, use the system name. The full host or system name is not required for a match.

Model

Model number on the device. This field matches on sub strings. The full model number is not required for a match.

Serial Number

Serial number on the device. Serial number requires an *exact* string match.

> **Note**
> Each filter value can only be applied once to a single rule.

Related Topics

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 Extreme Campus Controller.

To delete an adoption rule:

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

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

Related Topics

ExtremeGuest Integration

Use ExtremeGuest™ as an External Captive Portal Server to create and monitor External Captive Portals.

> **Note**
> The Extreme Campus Controller Network Access Control (NAC) Rules Engine is not invoked for clients on a WLAN Network that is configured to use the ExtremeGuest Server.
> The Network Access Server (RADIUS client) on Extreme Campus Controller handles the RADIUS transactions. RADIUS transactions are not relayed by NAC on Extreme Campus Controller.

ExtremeGuest integration within Extreme Campus Controller:

* To configure the ExtremeGuest server, select **Add**.

* To configure the ExtremeGuest captive portal settings, go to **Configure** > **Networks** > **Add**. Then, select **Enable Captive Portal**.

Related Topics

ExtremeGuest Server Settings

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 Extreme Campus Controller will attempt to authenticate an end user.

   Authentication Client UDP Port

   User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic.

   Shared Secret

   The password that is used to validate the connection between Extreme Campus Controller and the ExtremeGuest server.

   > **Mask** — Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

   Callback User Name

   User ID that Callback Manager uses to access the ExtremeGuest server.

   Callback Password

   The password that Callback Manager uses to access the ExtremeGuest server. The minimum password length is 6 characters.

   > **Mask** — Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Related Topics

Callback Manager

Callback Manager is an Extreme Campus Controller component that supports the integration of Extreme Campus Controller and ExtremeGuest. Callback Manager supports a Centralized site deployment only. It can report the following configuration changes to an ExtremeGuest server:

- Centralized site configuration changes
- AP configuration changes for APs associated with a Centralized site
- Network configuration changes for networks that are associated with a Centralized site.

> **Note**
> The ExtremeGuest user configures the report requests for each ExtremeGuest server.

Multiple servers are supported, and each server can request a different report.

To report configuration changes:

1. Callback Manager logs into the registered ExtremeGuest server over a secure http server (https):
2. Callback Manager receives the ExtremeGuest server request.
3. Callback Manager posts the requested configuration changes.
4. ExtremeGuest saves the changes.

Configure the User ID and password that Callback Manager uses to access the ExtremeGuest server on the **ExtremeGuest Server Settings** page.

If an ExtremeGuest server is unreachable, Callback Manager retries connection every few minutes. 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 Extreme Campus Controller restart. Once the appliance is restarted, Callback Manager continues to report changes that it had yet to report.

Related Topics

AAA RADIUS Authentication

You have options when configuring AAA Authentication:

- Use the local Network Access Control (NAC) to terminate or proxy a RADIUS authorization and accounting request.
- Use the local Network Access Server (NAS) to distribute RADIUS requests.

If you are going to authenticate with the Local Named Repository, opt for configuring authentication through the local NAC. If you are going to use an external RADIUS server, you have the option to configure the RADIUS server through the local NAC, through the local NAS, or connect directly to the RADIUS server, bypassing Extreme Campus Controller.

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

The RADIUS Authorization and Accounting transactions occur between the Network Access Server (NAS) on Extreme Campus Controller and the RADIUS server without involving NAC.

However, you have the option to configure Access Control Rules within the local NAC, making use of automated policy management. Access Control Rules enable you to apply network access permissions and restrictions based on defined rules. The rules can address network resources, a user's role or purpose in the organization, or the device type that is used to access the network. Network access control is dynamic. End-user network access can change as group associations change without a network administrator getting involved.

Regardless of the RADIUS configuration method you choose, you can easily configure RADIUS attributes and find support for RADIUS Change of Authorization (CoA).

Related Topics

Configure AAA Policy

You can create a AAA Policy that can be referenced through a WLAN Service, bypassing the local Network Access Control on Extreme Campus Controller.

> **Note**
> AAA Policy can only be configured for WLAN Networks requiring MACAUTH, External Captive Portal, or EAP.

To configure a AAA network policy:

1. Go to **Configure** > **Networks** > **WLANs** and select a network.

   AAA Policy is displayed for WLAN Networks that require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the Extreme Campus Controller. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal.

2. Select an **Auth Type**.

   The AAA Policy field displays.

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

4. Configure the following parameters:

   Name

   > Policy name.

   Authentication Protocol

   > Authentication protocol type for the RADIUS server (PAP, CHAP, MS-CHAP, or MSCHAP2).

   NAS IP Address

   > IP address of the Network Access Server (NAS).

   NAS ID

   > A RADIUS attribute that identifies the client to a RADIUS server. The NAS-Identifier can be used instead of an IP address to identify the client.

Call Station ID

Identifies a group of access points. The Call Station ID is often configured in a large network using an external NAC or RADIUS server. Possible values are:

- Wired MAC: SSID
- BSSID (APs supported on a Centralized site only)
- Site Name
- Site Name: Device Group Name
- AP Serial Number

	Note
	Call Station ID allows for Zone authentication with a Centralized site.

  - Site Campus
  - Site Region
  - Site City

Accounting Type

Determines when the appliance generates the accounting request. Valid values are:

- Start-Interim-Stop — Start record after successful login by the wireless device, interim record, and an accounting stop record based on session termination.
- Start-Stop — Start record after successful login by the wireless device user and an accounting stop record based on session termination.

The appliance sends the accounting requests to a remote RADIUS server.

Wait for client IP before starting accounting procedure

By default, the Accounting Start record is generated when the client is authenticated. Enable this setting to generate the Accounting Start record when the client acquires a non local IP address. Use this option for captive portals, which use RADIUS Accounting to learn of the client IP address before providing the landing page.

Accounting Interim Interval

The number of seconds (60-3600) between each interim update for a specific session. Default value is 60.

RADIUS Authentication Servers Mode

Select the availability behavior for RADIUS servers. Valid values are: **Failover** or **Load Balance**.

AAA Policy supports the ability to load balance RADIUS requests across target servers in a load-balancing pool. (A minimum of two servers is required.) Each client authentication session begins and ends on a single RADIUS server. The Extreme Campus Controller validates that each server can be reached and logs an alert when a server in the pool is unreachable. The server pool is readjusted based on the status of each server in the pool.

	Note
	Configure one server for both Accounting and Authentication purposes.

When this setting is set to **Failover**, a RADIUS request is sent to one server at a time:

- The RADIUS request is sent to the Primary server (based on the RADIUS server order in the AAA policy).
- When the Primary server is not accessible, the request is sent to the second server (the Failover server).
- When the Primary server is accessible, the request is automatically sent to the Primary server instead of the Failover server.

> **Note**
> The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

When this setting is set to **Load Balance**, a RADIUS request is sent in round robin fashion:

- When a RADIUS server is not accessible, Extreme Campus Controller stops sending requests to that server.
- When a server is accessible, the server is added to the pool of servers.

> **Note**
> The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

Include Framed IP

Select this option to include the FRAMED-IP attribute value pair in the RADIUS ACCESS-REQ message. You can include the user IP address in the RADIUS ACCESS-REQ through the FRAMED-IP attribute. This can extend user access reporting capabilities. Framed IP is supported by External Captive Portal only. Centralized Web Authentication does not support Framed IP.

RADIUS Authentication Servers

To add RADIUS servers for authentication, select **Add**. You can configure up to four RADIUS servers for authentication.

RADIUS Accounting Servers

To add RADIUS servers for accounting, select **Add**. You can configure up to four RADIUS servers for accounting.

Related Topics

RADIUS Settings

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 Extreme Campus Controller will attempt to authenticate an end user.

For Local Onboarding, use the **Retries** and **Timeout** values with the **RADIUS Server Health Check** parameters to detect RADIUS servers that are not responding and fail over to a second server if necessary. When Local Onboarding bypassed is enabled, all RADIUS requests are sent to one RADIUS server until it fails; then, the next RADIUS server is used.

Port

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.

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 248

Setting Default AAA Config on page 247

LDAP Configurations on page 251

Managing The Local Password Repository on page 254

Managing Captive Portal on page 257

Managing Access Control Groups on page 269

Access Control Rules on page 272

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 68: 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. Extreme Campus Controller 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 Extreme Campus Controller. Do not authenticate MAC address on the RADIUS server.

Related Topics

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, Extreme Campus Controller 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 69: 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 Extreme Campus Controller will wait for a response from the RADIUS server.
Authentication Timeout Duration	Determines a timeout value, in seconds, for the RADIUS server connection.
Authentication Retry Count	Determines the number of times Extreme Campus Controller will attempt to authenticate an end user.
Authentication Client UDP Port	User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic.
Proxy RADIUS Accounting Requests	Indicates that the RADIUS server will also handle RADIUS accounting requests.
Accounting Client UDP Port	UDP port number used for client accounting. User Datagram Protocol (UDP) needs only one port for full-duplex, bidirectional traffic.
Shared Secret	The password that is used to validate the connection between the client and the RADIUS server.
Mask	Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Related Topics

Advanced RADIUS Settings

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

Table 70: 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 71: 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 Administrator Password	Enter the administrator username and password used to connect to the LDAP server to make queries. The credentials only need to provide read access to the LDAP server. 802.1x authentication via LDAP requires domain membership. This requires authentication type to be NTLM and the Administrator Username to be in the format: `DOMAIN\USERNAME`.

Table 71: LDAP Configuration Settings (continued)

Field	Description
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.
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 72: 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.

Table 72: LDAP Schema Definition Settings (continued)

Field	Description
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.
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 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

Extreme Campus Controller gives you the option to store user accounts in a local password repository in place of configuring one or more remote RADIUS servers or remote LDAP servers to handle network authentication.

> **Note**
> The Admin account that you create here, from **Onboard** > **AAA** > **Local Password Repository**, applies to the local captive portal.
> This Admin account is separate from your Extreme Campus Controller system account. System accounts are managed from **Administration** > **Accounts**.

> **Note**
> When using local password authentication, you may also want to configure LDAP for additional user information.

Take the following steps to add new user accounts to the local repository:

1. Go to **Onboard** > **AAA** and select **Local Password Repository**.

   A list of user accounts displays. From here, you can search for, edit, delete, or add a new account.

2. To edit or delete an account, select an account row.

   The account settings display.

   - To edit the account, modify the account settings and select **Save**.

   - To delete the account, select **Delete**.

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

Related Topics

User Account Settings

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

Table 73: 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.

Table 73: User Account Settings (continued)

Field	Description
Last Name	User's last name.
Display Name	Name that displays on the user interface for the account. This can be the User name or something else.
Username	User name for the account.
Password Hash Type	Password hash function used for password hashing.
Password	Password for the account. Alphanumeric value, minimum of 6 characters. The default captive portal password is `Extreme@pp`.
Description	Text description of user account.

Related Topics

Managing The Local Password Repository on page 254

Certificates

To ensure a secure website that takes advantage of encryption, Extreme Campus Controller uses browser certificates for website security and RADIUS Server certificates for certificate-based authentication to the network and for access to a captive portal. The browser certificate ensures security between the wireless clients and a VLAN, and the RADIUS server certificates ensure security between the RADIUS server and Network Access Control.

Both types of certificates offer the option to generate a new certificate or use a certificate and key file that you have saved. You can also reset the network interface to the default certificate and key, which yields a Self-Signed certificate.

Extreme Campus Controller offers a factory installed self-signed certificate, which is used by the user interface HTTP Server to terminate the HTTPS browser requests served on port 5825. The certificate common name is *Network Services Engine*.

Related Topics

Generate Browser Certificates on page 255

Generate RADIUS Server Certificates on page 256

AAA Certificate Authorities on page 257

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 Extreme Campus Controller to the default configuration of the Self-Signed certificate.

   > **Note**
   > When certificates are applied or reset on the Admin topology, a server restart is triggered, and the browser loses connectivity with the server for a few seconds. When certificates are applied or reset on System topologies where **Management Traffic** is enabled, the server is also restarted.

Related Topics

   Certificates on page 255

Generate RADIUS Server Certificates

RADIUS server certificates ensure encryption between the RADIUS server and Extreme Campus Controller. To generate and load a certificate, take the following steps:

1. Go to **Onboard** > **AAA** and select **Manage Certificates**.
2. Under RADIUS Server Certificate, select **Update Certificate**.
3. Select the Certificate option:

   - **Generate a new unique private key and certificate**

     This option generates and loads a Self-Signed certificate.

   - **Provision a private key and certificate from files**

     This option loads the key and certificate from a Certificate Authority. Select this option, then do the following:

     a. Select **Choose File** and navigate to the Private Key file.
     b. If the Key file is password protected, check the box and provide the password.
     c. Select from the list of possible certificate files.
     d. To add certificate files, select **Add Files**, navigate to the saved certificate file, and select **Open**.

4. Select **Save** to save your changes and close the dialog.

Related Topics

Certificates on page 255

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 Extreme Campus Controller, select **Add CA Certificates** and navigate to the certificate file. Then, select **Open**.
4. To add URLs to the Certificate Revocation List (CRL), select **Add URL**, and provide a valid CRL.
5. Check the box to allow expired CRLs to be used to validate certificates.

Related Topics

Certificates on page 255

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/administration`.

Related Topics

Portal Website Configuration on page 257
Portal Network Configuration on page 266
Portal Administration Configuration on page 267

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 74: 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 75: 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 207.
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 207.
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 207.
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 207.
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 207.
Provider 1 Registration	Select this option to use credentials from a custom application that you configure. See Walled Garden Rules on page 207.
Provider 2 Registration	Select this option to use credentials from a custom application that you configure. See Walled Garden Rules on page 207.

> **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 Extreme Campus Controller with a higher level of user information by obtaining information from the end user's third-party application account instead of relying on information entered by the end-user.

- It provides an easier registration process for the end user. Extreme Campus Controller retrieves the public information from the end user's third-party account and uses that information to populate the name and email registration fields.

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 Extreme Campus Controller receives from the third-party application.

- The end user grants Extreme Campus Controller access to the third-party information and is redirected back to the captive portal where they see a "Registration in Progress" message.

- The third-party application provides the requested information to Extreme Campus Controller, which uses it to populate the user registration fields.

- The registration process completes and network access is granted.

Third-party Registration Requirements

Third-party captive portal registration requires the following:

- The Extreme Campus Controller Access Control engine must have Internet access in order to retrieve user information from the third-party application.

- The Extreme Campus Controller Access Control Unregistered access policy must allow access to the third-party application site (either allow all SSL or make allowances for application servers).

- The Extreme Campus Controller Access Control Unregistered access policy must allow access to HTTPS traffic to the third-party application OpenID servers.

- A Unique third-party application must be created on the third-party application Developers page.

- The Portal Configuration must have the third-party application enabled and include the third-party application Application ID and Secret.

Authenticated Portal: Authenticated Web Access

Table 76: 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 77: 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 77: 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 78 to customize your captive portal.

Table 78: 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 78: 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 78: 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. Select an existing portal or select **Add**.

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

Table 79: 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, Extreme Campus Controller can assume that the end user has network access and redirects the end user out of the captive portal. Use an internal image that end users don't have access to until they are accepted. It is recommended that the test image URL is a link to an SSL site, because when the captive portal is configured for `Use HTTPS`, the browser will not allow the attempt to an HTTP test image site. It is also recommended that the captive portal policies (typically the Unregistered and Quarantine policies) are configured to deny HTTPS traffic. This prevents the test image connection attempt from successfully completing and moving the end-system out of the captive portal prematurely. If access to the test image is available, the user may experience the captive portal reverting to the "Click here to access the network page", and then upon selecting the link, returning to the previous page based on their state. This behavior continues until the user is finally accepted on to the network.
Test Image URL	Specify the URL for the immediate redirection. See Redirect User Immediately.
Redirection	See Redirection.
Destination	When Redirection field is set to **URL**, specify the URL for the web page redirection here.
Client Auto Log in Handling	Extreme Campus Controller supports auto-detection of a captive portal. Valid values are: • Redirect — Auto-detection is enabled and client is automatically redirected to the captive portal. This is the default setting. • Hide — Disables auto-detection of captive portal.

Portal Administration Configuration

Configure settings for the Registration Administration web page and grant access to the page for administrators. The Registration Administration web page allows Helpdesk and IT administrators to

track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network.

1. Go to **Onboard** > **Portal**.
2. Select an existing portal or select **Add**.
3. Configure the following parameters on the **Administration** tab.

Table 80: 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 268

Login Configuration Settings

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

Table 81: 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 267

Managing Access Control Groups on page 269

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 user group. Configure groups to be used with access control rules. Extreme Campus Controller provides a set of default system groups with your installation to simplify the group set up process.

To manage the list of groups:

1. Go to **Onboard** > **Groups**.

   A list of configured groups displays. From here, you can search for a group, edit group settings, delete a group, or add a new group.
2. To edit or delete a group, select a group row.

   The group settings display.
   - To edit a group, modify the group settings and select **Save**.
   - To delete a group, select **Delete**.
3. To add a new group, from the **Access Control Groups** page, select **Add** and configure the group settings.

Related Topics

Access Control Group Settings

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

Table 82: Access Control Group Settings

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

Table 82: 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 User Groups only** — Specify whether to match any or match all of the LDAP attributes. Valid values are: • Match All • Match Any
Group Entries	A list of entries for the group. Use the **Search** field to search for an entry.

Related Topics

Working with Group Entries

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.

   Extreme Campus Controller prompts you to open the new group.
5. Add, remove, or edit group entries and settings as necessary.

Related Topics

Access Control Group Settings on page 269
Working with Group Entries on page 270

Default Groups Provided with Your Installation

The following Access Control system groups are provided with the Extreme Campus Controller installation by default.

- Blacklist. A list of MAC addresses that are prohibited from accessing the network.
- Registered Guests. A list of MAC addresses that have been granted access to the network via the Guest captive portal.
- 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 Extreme Campus Controller 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 269
Access Control Group Settings on page 269

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.

Extreme Campus Controller 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 Extreme Campus Controller installation provides the following default system rules:

- Catch-All rule. End-systems that do not match any of the defined rules are assigned the default Catch-All rule. The Default Catch-All rule assigns the Enterprise User policy role by default, which allows full network access. The policy role assigned by this rule is configurable (You can edit the rule and change the "Accept Policy" field value.)
- Blacklist. End-systems with a MAC address that is a member of the Blacklist group are denied network access. They are assigned the Quarantine policy role. The Quarantine policy denies all traffic by default. Go to **Policy** > **Roles** to configure the Quarantine policy definition.

Related Topics

Configuring Network Policy Roles and Dynamic Access Control

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 Extreme Campus Controller installation provides the following default system rules:
>
> - Catch-All rule. End-systems that do not match any of the defined rules are assigned the default Catch-All rule. The Default Catch-All rule assigns the Enterprise User policy role by default, which allows full network access. The policy role assigned by this rule is configurable (You can edit the rule and change the "Accept Policy" field value.)
>
> - Blacklist. End-systems with a MAC address that is a member of the Blacklist group are denied network access. They are assigned the Quarantine policy role. The Quarantine policy denies all traffic by default. Go to **Policy** > **Roles** to configure the Quarantine policy definition.

Related Topics

Add Policy Roles on page 214

Managing Access Control Groups on page 269

Managing Access Control Rules on page 274

Rule Settings on page 275

Access Control Rules on page 272

Managing Captive Portal on page 257

Managing Access Control Rules

An Access Control Rule is used to further define an end user's network access based on the groups and policy roles with which the end user is associated.

Go to **Onboard** > **Rules**.

A list of configured rules displays. From here, you can edit rule settings, delete a rule, or add a new rule.

- To edit a rule, select a rule from the list and click ✎. Modify the rule settings and click **Save**

- To delete a rule, select a rule from the list and click 🗑. Or, edit the rule to open the **Settings** dialog and click **Delete**.

- To add a new rule, from the **Rules** page, click **Add** and configure the rule settings.

Related Topics

Access Control Rules on page 272

Configuring Network Policy Roles and Dynamic Access Control on page 272

Default Rules for Captive Portal on page 275

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 select **Save**.

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

Table 83: Access Control Rule Settings

Field	Description
Name	Rule name. You cannot change the name of default rules that are provided with Extreme Campus Controller.
Rule Enabled	Indicates if the rule is enabled. You cannot disable default rules that are provided with Extreme Campus Controller.
Conditions **Note:** • If you select **Any**, then the criteria is ignored during the rule match process. • If you select the **Invert** check box, it is considered a rule match if the end-system *does not* match the selected value.	
User-Group	The user group that you configured. Users in this group are affected by the rule. User groups limit a user's access based on the LDAP, RADIUS, or Username group to which they are assigned.

Table 83: Access Control Rule Settings (continued)

Field	Description
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 86.
Portal	Associate a captive portal with a rule.

Related Topics

Tools

Workflow

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

Go to **Tools** > **Workflow** to begin.
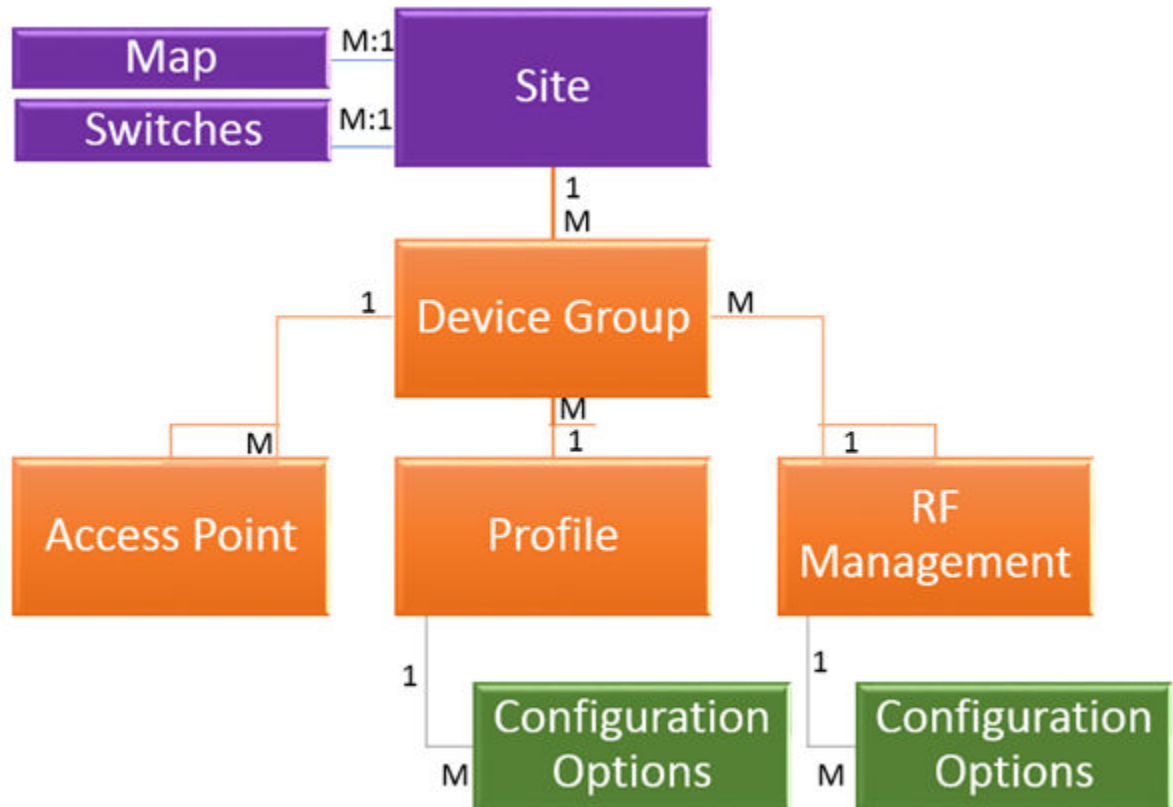
Figure 49: Extreme Campus Controller Component Relationship

Related Topics

Navigating Extreme Campus Controller Using Workflow

The following component types are displayed when you access **Tools** > **Workflow**: Site, Profile, Role, and Network.

Alternatively, you can use the **Search** field to search for any component.

The **Workflow** pane lists all components that are available in Extreme Campus Controller. You can add and delete components using Workflow.

Select an icon on the **Workflow** page to display a list of available components and navigate through the component hierarchy.
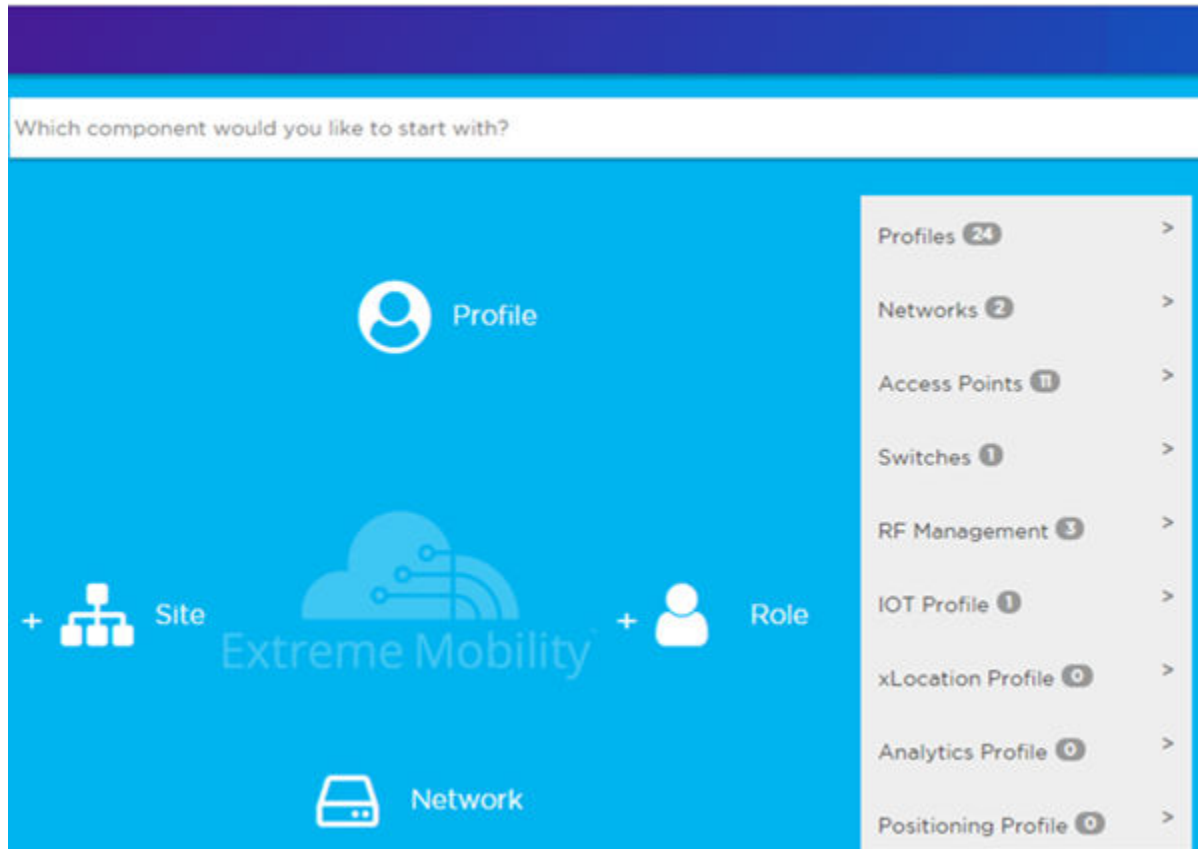
Figure 50: Workflow Main Page

Related Topics

How to Navigate Using Workflow

Go to **Tools** > **Workflow** to navigate Extreme Campus Controller accessing components. The following example illustrates the relationship between Extreme Campus Controller components, and it demonstrates how to easily access each component using **Workflow**.

1. Select the **Site** icon on the **Workflow** page to display a list of available sites.

    > **Note**
    > If there is only one available component of that type, the component details or configuration page displays instead of a list of specific components.

2. Select a specific site from the **Site** list.

A site has the following associated components: Access Point, Device Group, and Switch.
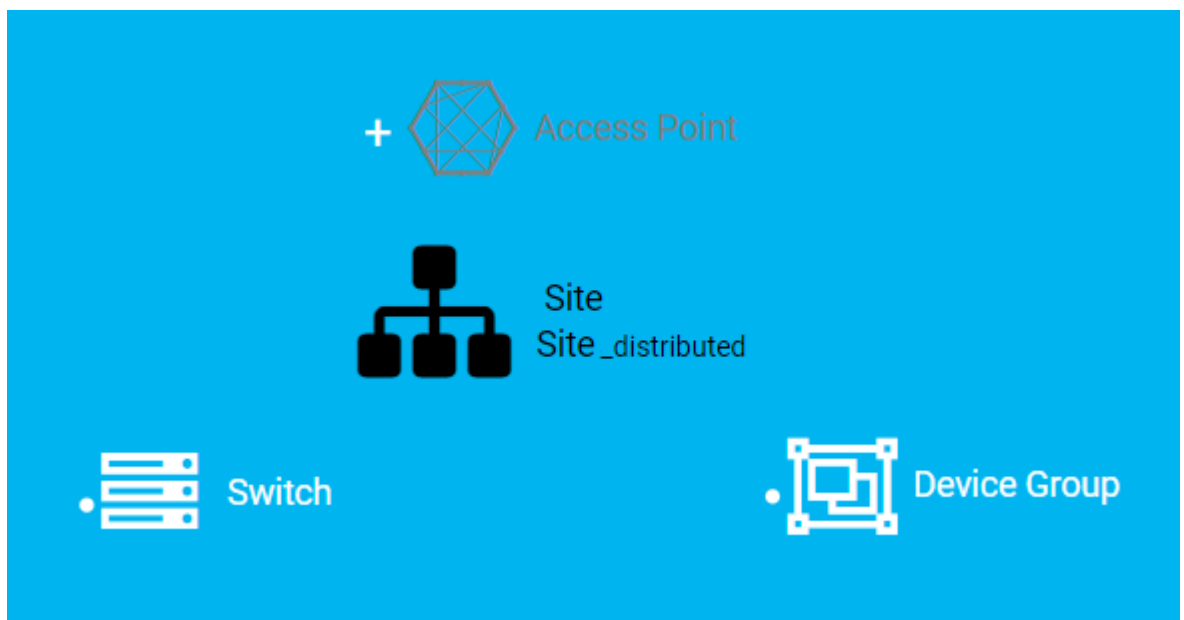
Figure 51: Site with associated components

Figure 51 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.
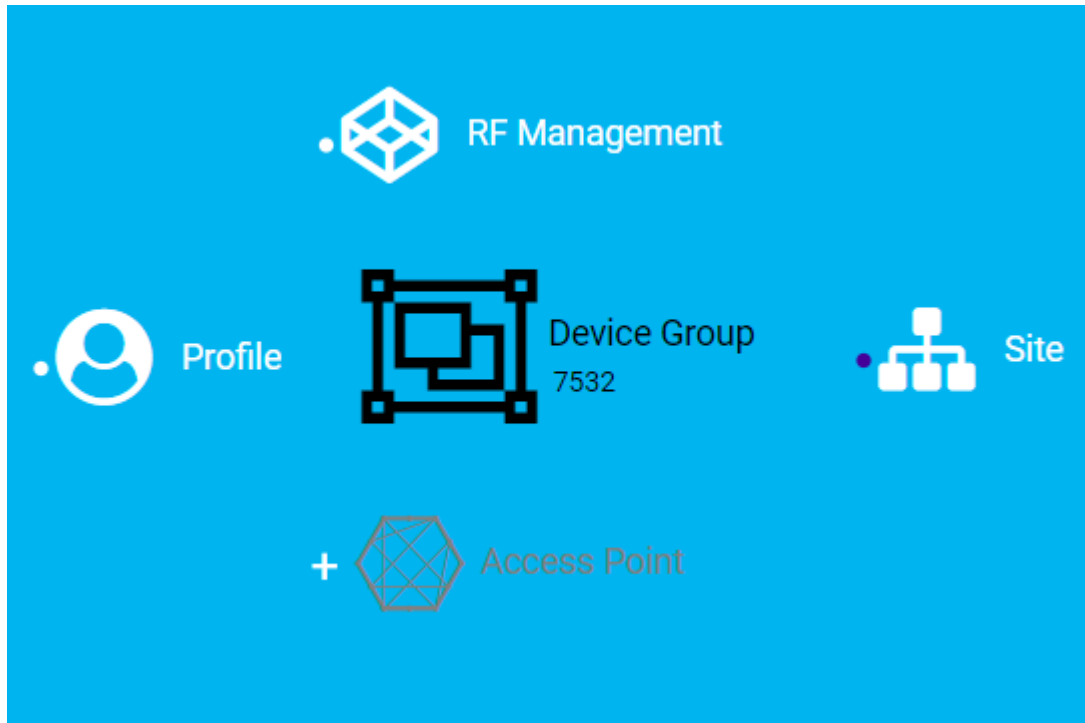
Figure 52: Device Group with associated components

- 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 154.

6. Each device group has a single profile. Click the **Profile** icon to display the configuration items associated with that profile.
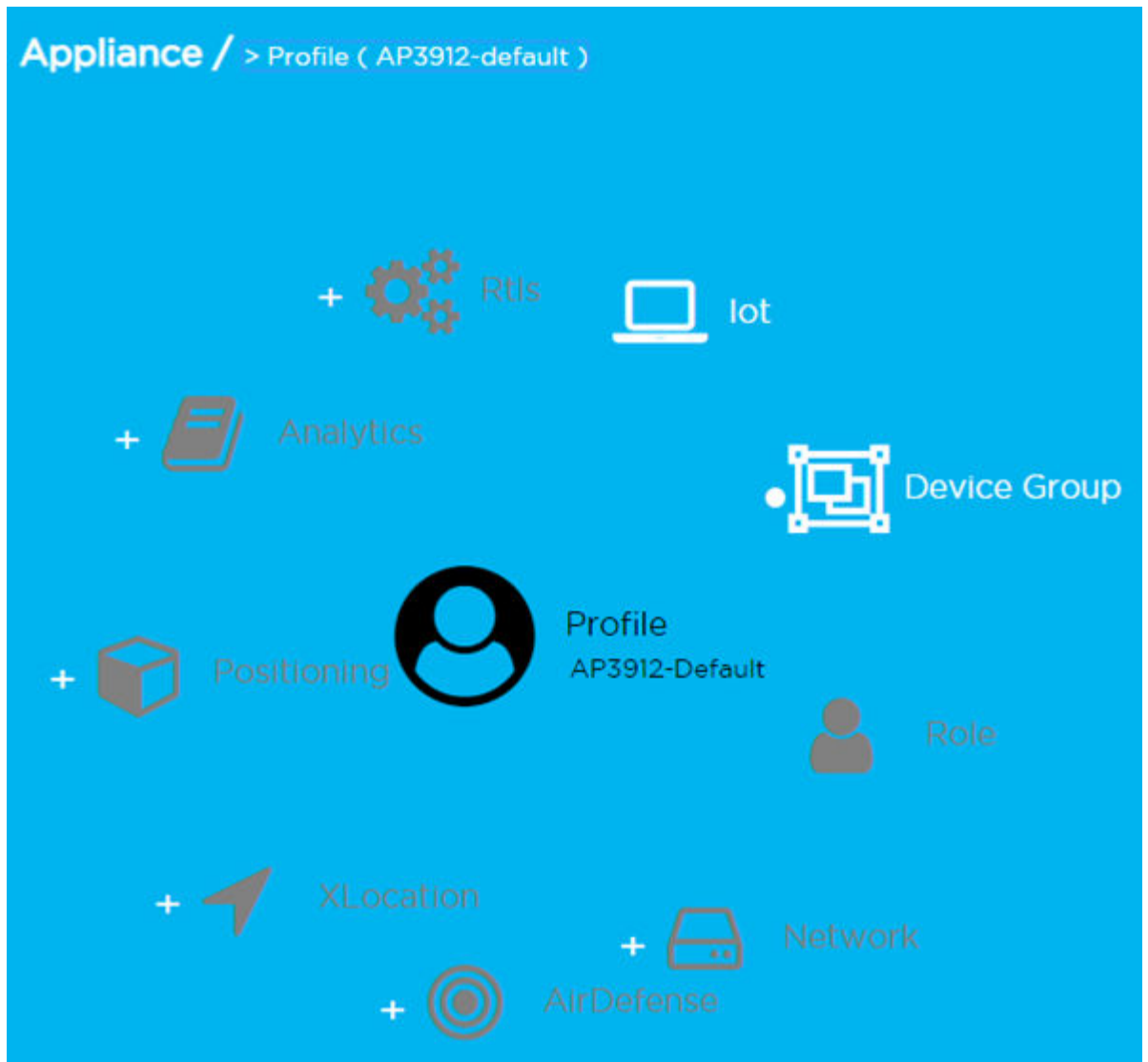
Figure 53: Profile with associated components

> **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 Extreme Campus Controller. Use the Workflow breadcrumbs to move backwards in the hierarchy, Alternatively, you can use the **Search** field on the **Workflow** page to search for a component.

Related Topics

Adding Components from Workflow

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**.
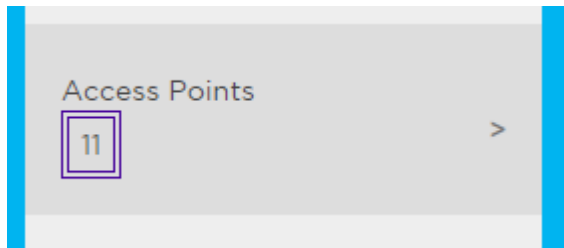
Figure 54: Workflow Pane APs

2. Select the plus sign.
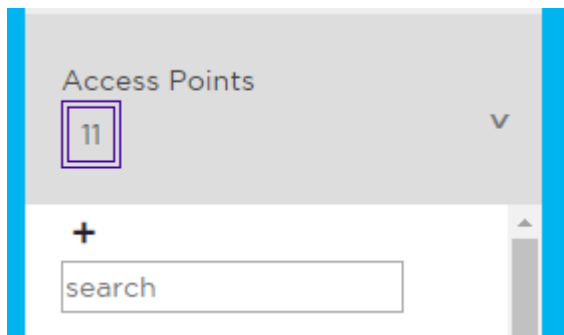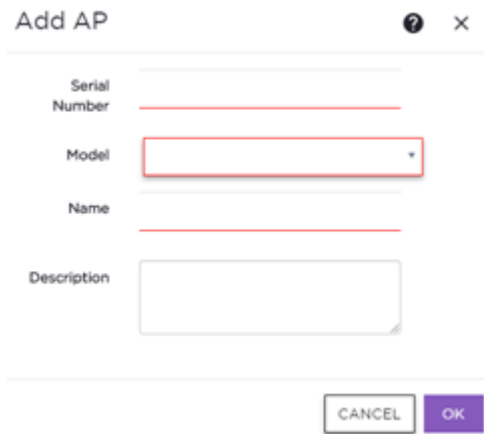
Figure 55: Adding APs from Workflow Pane

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 56: 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 155 for instructions on configuring the AP radio settings.

Related Topics

   Configure AP Radio Settings on page 155

Deleting Components from Workflow

You can delete Extreme Campus Controller components from **Workflow**:

From the **Workflow** pane:

1. Click the drop-down arrow under a component type and select an item from the list.

2. Click 🗑.
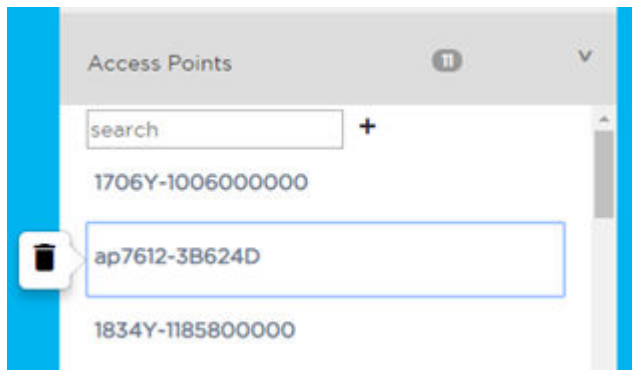
A confirmation dialog displays.

Figure 57: 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 95
WLAN Service Settings on page 180

Logs

The log messages contain the time of event, severity, source component, and any details generated by the source component. Log messages are presented under the following report tabs:

- Events
- Station Events
- Audit
- AP Logs
- AP Upgrade Report on page 292

Working with the logging page:

- Select the plus icon next to each log entry to expand, showing entry details.
- Highlight log entries and (using shortcut keys) copy/paste entries into a third-party application.
- Create Date/Time filters to display entries that were logged around that time. Entries with the approximate time are displayed.

Related Topics

Understanding Date and Time on page 25
System Logging Configuration on page 319
Set a Logging Filter on page 291

Advanced Filtering

Extreme Campus Controller offers a Query Builder to filter logs, enabling you to find records more easily, improving efficiency of diagnostics. Perform an advanced query over Events, Audit log, AP logs, and Station events. The saved queries are persistent to each individual Log tab.

Related Topics

Build a Query for Logs on page 287

Build a Query for Logs

Take the following steps to build a customized query, filtering data in the **Logs** page:

1. To access the **Logs** page:

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

2. To open Query Builder, select **Launch Query Builder**.

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

    -   AND

    -   OR

    > **Note**
    > AND is the only supported condition within a group.

3. To add a condition, select **+ Condition**.
4. From **Source Field**, select a value that represents a column used in the query.
5. Select the **Operator**.

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

    -   Equals

    -   Not Equals

    -   Contains

    -   Greater Than

    -   Less Than

    -   Less or Equals

    -   Greater or Equals

6. Under **Search Condition**, provide the value that you are searching for.

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

    -   Select **+** to add conditions.

    -   Select **-** to remove conditions.

7. To add another condition row, select **+** .
8. **Group** — Each group has conditions joined by the selected operator. You can add additional groups or add conditions to the group.
9. To run the query, select **Execute**.

    The query is automatically saved.

    > **Note**
    > Query Builder generates a Pandas query syntax. The syntax preview is displayed at the top of the **Query Builder** dialog. For saved queries:
    >
    > -   Select 👁 to view the Pandas query.
    >
    > -   Select 🗐 to copy the Pandas query to the clipboard.

Figure 58: Query Builder: Events Query Type Info

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

Figure 59: List of saved queries

Query Builder actions:

- **New**. Provide a name, and add a blank dialog so you can create a new query. There is a limit of 10 saved queries per user, per grid. After the 10-query limit has been reached, the **New** button is unavailable.
- **Rename**. Rename an existing query.
- **Delete**. Delete the query that is currently displayed.
- **Close**. Close the Query Builder dialog. If you close Query Builder without running the query, your query details are deleted.

- **Reset**. Close the Query Builder dialog and saves the current query. The next time you open Query Builder, this query will display. Available after you run a specific query.
- **Execute**. Run the query and saves it.
- **Save**. Save changes without executing the query. Save is only visible when changes have been made.

Related Topics

Query Builder on page 52

Build a Query for Devices or Clients on page 53

View Events Log

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

Events log files include the following information:

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

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

Related Topics

System Logging Configuration on page 319

Understanding Date and Time on page 25

Set a Logging Filter on page 291

View Station Logs

If configured to do so, Extreme Campus Controller 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**
> Extreme Campus Controller provides station event history for active stations. You can also search for inactive stations using a MAC address or user name.

Related Topics

System Logging Configuration on page 319
Understanding Date and Time on page 25
Set a Logging Filter on page 291

View Audit Logs

Extreme Campus Controller logs all configuration changes made by administrators and system messages related to end-system activity. You can view a record of the changes and messages in the user interface.

Audit log files include the following information:

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

To view audit 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, Extreme Campus Controller 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 time stamp
- 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

Set 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 Extreme Campus Controller:

1. Go to **Tools** > **Logs**.
2. To display the **Start Date/Time** dialog, select **Change**.
3. From the Time field, specify the hour and minutes and select **AM** or **PM**.
4. In the Date field, use the arrows to navigate to the month, then select the calendar day.
5. Select **OK**.

Entries with the approximate time are displayed.

NEW! AP Upgrade Report

The AP Upgrade Status Report provides the progress status of the AP upgrade request. View information on the AP group or drill down to view the status of each individual AP in the group.

The AP group is identified by the Upgrade Request Time. Each request is considered a group. A group must consist of APs that support the same firmware version. For example, currently all AP39xx series APs support firmware version: `10.51.15.0002.img` and all 11ax APs support firmware version: `7.5.0.0-005R.img`.

Each Extreme Campus Controller release includes default AP firmware versions for the supported APs. You can install additional firmware versions if necessary. Before initiating an AP Upgrade Request, verify that the AP firmware is installed on Extreme Campus Controller.

For each group, the report displays the upgrade status percentage, the estimated completion time, and the actual completion time. To display this same information for each AP in the group, select the group.

Figure 60: AP Upgrade Report

The AP upgrade status is color coded:

- Green indicates the percentage completed.
- Mustard indicates the percentage scheduled.
- Blue indicates the percentage in progress.
- Red indicates the percentage failed.

The AP Upgrade Status Report is available on the following workbenches:

- **Administration** — Go to **Administration** > **System** > **Software Upgrade**. Scroll down to **AP Images** and select **Upgrade Status**.
- **Tools** — Go to **Tools** > **Logs** > **AP Upgrade Reports**.

> **Note**
> Advanced Query and filtering from the **Log** workbench are not available for the AP Upgrade Report.

The AP Upgrade Request does not provide a history of upgrades. If multiple upgrades are requested for the same AP, only the most recent upgrade request is shown. To view event information for the AP Upgrade Request, configure the System Log Level to `Information`. Go to **Administration** > **System** > **Logs**.

Select ≡ to configure the column display, refresh the display, or export the data in .csv.

Related Topics

Diagnostics

Extreme Campus Controller offers diagnostic tools to help you troubleshoot your network. Go to **Tools** > **Diagnostics**.

Related Topics

NEW! Network Utilities

Use wireless controller utilities to test a connection to the target IP address (or Fully-Qualified Domain Name) and record the route through the Internet between your computer and the target address. You can also use controller utilities to capture exception traffic, which can be useful for network administrators when debugging network problems.

Configure the following parameters:

Table 84: Network Utilities

Field	Description
Target IP Address or Fully-Qualified Domain Name (FQDN)	IP address or FQDN for the test target.
Use specific source interface	Indicates if a specific interface will be selected for the test. Select the interface from the Select Interface field. When this option is cleared, Extreme Campus Controller runs the test based on the interface selected in the routing table.
Select Interface	Used with Specific Source Interface option. See list of possible interfaces on the **Interface** tab.
Ping	Initiate the Ping network utility to determine reachability of the IP address or FQDN that you specify.
Trace Route	Initiate the Trace route command, which traces the path of a packet from Extreme Campus Controller to the IP address or FQDN that you specify. It lists the routers it passes until it reaches its destination, or fails to. It also indicates the length of each hop.

Related Topics

TCP Dump Management

Table 85: 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 Extreme Campus Controller in a redundant configuration, providing connectivity to two different switch stacks for the same port function. Extreme Campus Controller 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 Extreme Campus Controller and its APs interact. The attributes of a topology are: VLAN ID, Port, IP address, Mode, and certificates. To add an interface, click **Add**.

Static Routes

Use static routes to set the default route of the Extreme Campus Controller 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 86: 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 Extreme Campus Controller management port.
VLAN ID	ID for the virtual network.

Table 86: 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 Extreme Campus Controller for the interface.
Enable Device Registration	Enable or disable AP registration through this interface. When enabled, wireless APs use this port for discovery and registration. Other Extreme Campus Controllers can use this port to enable inter-Extreme Campus Controller device mobility if this port is configured to use SLP or the Extreme Campus Controller is running as a manager and SLP is the discovery protocol used by the agents.
Management Traffic	Enable or disable Management Traffic through this interface. Enabling management provides access to SNMP (v1/v2c, v3), SSH, and HTTPs management interfaces.
MTU	Maximum Transmission Unit (MTU). Standard is 1500 bytes. Fixed value.
Layer 3	
IP Address	For an Admin topology, the Layer 3 check box is selected automatically. The IP address is mandatory for a Physical topology. This allows for IP Interface and subnet configuration together with other networking services.
CIDR	CIDR field is used along with IP address field to find the IP address range.
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 Extreme Campus Controller is used for managing IP addresses.

Related Topics

Multiple LAG Interface Support

Extreme Campus Controller supports redundant configurations where the appliance provides connectivity to two switch stacks for one port function. On the **L2 Ports** pane, you can configure Extreme Campus Controller attachment through a LAG to one switch, or attached to two separate

switch stacks, forming a Multiple Link Aggregation Group (MLAG). An MLAG joins two or more interfaces in the same Link Aggregation Group.

> **Note**
> Multiple Link Aggregation Group (MLAG) is supported on hardware appliances E1120, E2120, and E3120. MLAG is not supported on Extreme Campus Controller virtual appliances (VMware or HyperV based platforms).

Add a Static Route

Static Routes define the default route to Extreme Campus Controller for legitimate wireless traffic. You must be a system administrator to add a static route.

> **Note**
> Static Routes affect the settings for the Default Gateway IP address under **Host Attributes**. Adding a default static route (0.0.0.0/0) changes the Default Gateway IP address.

To add a static route, take the following steps:

1. Go to **Administration** > **System**.
2. Under Static Routes select **Add**.

   The **Create New Static Route** dialog displays.
3. Configure the following parameters:

Table 87: Static Route Parameters

Field	Description
Destination	IP address of the destination Extreme Campus Controller.
CIDR	CIDR field is used along with IP address field to find the IP address range.
Gateway	Gateway address of the Extreme Campus Controller 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. Extreme Campus Controller has lost connectivity.

> **Note**
> Network Time settings on each appliance of an Availability Pair must be identical for the configuration update process to be successful.

Software Upgrade

The following processes are components of the software upgrade process:

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

> **Note**
> Extreme Campus Controller supports Campus/Centralized sites only. During system upgrade to Extreme Campus Controller, the upgrade process checks for Distributed sites. If Distributed sites are part of the instance configuration, the upgrade process will abort and log the following:
>
> - <date> ERROR: Upgrade aborted due to the presence of a Distributed site
> - <date> ERROR: System upgrade failed
>
> After the upgrade process aborts, the system is retained at its current revision. The configuration state is not affected. Support for Distributed sites remains in ExtremeCloud Appliance v4.76.02 and later.

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 301.

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.

> **Note**
> It is a best practice to set up a scheduled backup for all managed appliances.

On-demand backups can only be stored locally, while scheduled backups can be stored on a mounted flash drive or on a remote server.

Related Topics

Configure a Backup Schedule

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

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 Extreme Campus Controller, select it and take one of the following actions:

⊕ Copy Backup

⟲ Restore system with backup file

⬜ Copy backup file to remote system.

⬇ Download backup file to a local computer

🗑 Delete backup file.

> **Note**
> The restore process checks for Distributed sites. If Distributed sites are part of the instance configuration, the restore process will abort and log the following:
> - <date> ERROR: Restore action aborted due to the presence of a Distributed site

Related Topics

Copy Backup on page 301
Remote Server Properties on page 303

Copy Backup

To copy a backup image to Extreme Campus Controller, configure the following parameters:

Upload Method

Method used to upload file to appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.
- FTP — Indicates to upload from the corresponding server.
- SCP — Indicates to upload from the corresponding server.

When the Upload Method is **FTP** or **SCP**, configure the server properties.

Copy Image from Local Drive

When the Upload Method is **HTTP**, drag image onto Extreme Campus Controller or select field to navigate to local file directory.

Related Topics

Remote Server Properties on page 303
Upgrade Software on page 301
Restoring a Backup File on page 300

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 Extreme Campus Controller software.

There is more than one way to put the upgrade image on Extreme Campus Controller:

- Select a local upgrade image. Or
- Click 🔵 to display the **Copy Upgrade Image** dialog. For more information, see Copy Upgrade Image on page 302.

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

To copy an upgrade or backup image to Extreme Campus Controller, configure the following parameters:

Image Type

Indicates the type of image file used. Valid values are:

- Upgrade
- Backup

Destination

Destination of the uploaded image file:

- Local
- Flash (The Flash drive must be mounted.)

Upload Method

Method used to upload image file to appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.
- FTP — Indicates to upload from the corresponding server.
- SCP — Indicates to upload from the corresponding server.

When the Upload Method is **FTP** or **SCP**, configure the server properties.

Copy Image from Local Drive

When the Upload Method is **HTTP**, drag image onto Extreme Campus Controller or select field to navigate to local file directory.

Select Image

Due to a storage space limitation, Extreme Campus Controller limits the number of locally available upgrade archives. If necessary, you can delete an older image before you upgrade to the latest image. To delete an image from Extreme Campus Controller, 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 88: Remote Server Properties

Field	Description
Upload Method	Indicates the transfer protocol to use to transfer the backup file. Valid values are: Local, FTP (File Transfer Protocol) or SCP (Secure Copy Protocol).
Server IP	IP Address of the server.
Username	User name to log into the server.
Password	Password to log into the server.
Directory	Destination or source location of file on the server.
Filename	Name of the backup file.
Destination	Destination directory for copied backup file.

Select **OK** to initiate the copy action.

Related Topics

Configuring an Upgrade Schedule

After you have the image file on Extreme Campus Controller, you can upgrade right away or schedule an upgrade.

To schedule an upgrade:

1. Go to **Admin** > **System** > **Software Upgrade**.
2. In the Upgrade section, from the Upgrade field, select **Schedule** and select **Configure Schedule**.
   The **Schedule Upgrade** dialog displays.
3. Configure the following parameters:

   Upgrade Image

   Name of the upgrade image file.

   Backup Filename

   Name of the backup image file.

   Backup Location

   Indicates where to save the backup image file. Local is currently the only supported value. Save the backup image locally on Extreme Campus Controller.

   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. Select **Schedule**.

Related Topics

Software Upgrade on page 299

View Upgrade Logs

The following Extreme Campus Controller software upgrade activity is displayed on the **Software Upgrade** tab under **Logs**.

1. Go to **Administration** > **System** > **Software Upgrade**.
2. Scroll down the page and select **Logs +**.

The following upgrade information is available:

- Upgrade History
- Upgrade Details
- Restore Details

3. Select the appropriate tab to view information.

Related Topics

Software Upgrade on page 299

NEW! Upgrade AP Images

Extreme Campus Controller is released with the latest AP images for each supported AP Type. When you upgrade Extreme Campus Controller, in a stand-alone deployment, the connected access points are automatically upgraded to the latest firmware image. In a High-Availability deployment, you must manually upgrade the APs. You can also upgrade additional devices without upgrading the controller.

To upgrade APs:

1. Verify that the upgrade image file is installed on Extreme Campus Controller for the selected AP platform. If necessary, install the AP image file onto the controller.
2. From the **Access Points List**, select one or more APs to upgrade.
   - You can upgrade from the **Access Points List** associated with a site. Go to **Monitor** > **Sites**. Select a site and select the **Access Points** tab. Or,
   - Go to **Configure** > **Devices** > **Access Points**.
3. Go to the **AP Upgrade Status Report** to view progress of the upgrade.

Consider the following when upgrading AP images:

- Selected APs must support the same upgrade image file. AP39xx series and Wi-Fi 6 APs have different firmware images; therefore they cannot be selected for upgrade together. Instead, create two AP upgrade requests:
  - The ExtremeWireless AP39xx Series Access Points support the same firmware image file. They can be upgraded together.
  - The ExtremeWireless Wi-Fi 6 Access Points support the same firmware image file. They can be upgraded together.
- The APs must be connected to Extreme Campus Controller. If the AP is in a disconnected state, the upgrade is scheduled, but cannot complete until the AP discovers Extreme Campus Controller .
- Each Extreme Campus Controller release includes the latest AP image files for the supported access points. A stand-alone deployment automatically updates the AP firmware to the latest release. For a High-Availability deployment, upgrade all connected APs from the **Access Point List**.
- You can monitor the AP upgrade process from the **AP Upgrade Report**.
- To display AP Upgrade events, from the **Events** tab, configure your SysLog to *Informational*.

Related Topics

Install AP Firmware Image

To upgrade AP image files, do the following:

1. Go to **Administration** > **System** > **Software Upgrade**.
2. Scroll down the page to **AP Images**.
3. Select an AP Platform.

   | Note
   | The action to upgrade an AP3916-Camera, applies to all APs with onboard cameras. The camera upgrade is not limited to a single device.

4. To upload image from local drive:

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

   Available images are listed. Select ↻ to refresh the list. When you have more than one image file, you have the option to **Set Default AP Image** and **Delete AP Image**.

5. Select **Upgrade Status** to view the AP Upgrade Status.

Related Topics

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 Extreme Campus Controller shuts down, then reboots. A warning message is displayed, asking you to confirm your selection.

Halt System

The system enters the halted state, which stops all functional services, the application, and associated wireless APs. A warning message is displayed, asking you to confirm your selection. To restart the system, the power to the system must be reset.

Web Session Timeout

Determines the web session inactive window before the session times out. Enter the value as hours : minutes. The range is 1 minute to 168 hours (7 days).

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 Extreme Campus Controller that provides detailed configuration for logging, the ability to capture packets, and debugging information. Customers can configure logging via this interface when debugging. The default login credentials are `admin/Extreme@pp`.

The Web App displays detailed information in the following categories:

- Status
- Diagnostics
- Log Files
- Downloads
- Utilities

External Flash

Physically connect an external device to the Extreme Campus Controller and then mount the device to display memory usage and capacity. Mounting a device makes the flash device that has been inserted into the Extreme Campus Controller available for use.

Flash devices must be formatted in FAT32. Only the first partition of the flash device is used by the Extreme Campus Controller. Files must reside in the root directory. The Extreme Campus Controller

software cannot operate with files in sub-directories. The Extreme Campus Controller supports only one USB device at a time, regardless of which USB connector the device is connected to. If you connect more than one USB device at a time, the system returns an error.

> **Note**
> Format flash devices as non-bootable. The Extreme Campus Controller may experience difficulty rebooting when connected to a bootable formatted flash device.

Tech Support

Generate a tech support file for troubleshooting. Select the file criteria: **Extreme Campus Controller**, **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 ![download icon].

Availability

Extreme Campus Controller 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:

- Extreme Campus Controller directly balances capacity allocations across both appliances in an Availability Pair. Adoption Capacity is additive. For example, to support a 600 AP Capacity, you can purchase a 500 Device Capacity and a 100 Device Capacity. The Availability pair shares the installed capacity to the 600 limit. You can enter the entitlements on either system in the pair. However, when purchasing capacity license SKUs, make sure that none of the license blocks exceed the maximum adoption capacity for any individual system.
- Availability pair can be configured only within the same Extreme Campus Controller models.
- Enable and configure NTP: Network Time settings on each appliance of an Availability Pair must be identical for the configuration update process to be successful.
- Use the Network Health chart on the Extreme Campus Controller Dashboard to monitor the Availability Link Status and the Synchronization Status for an Availability Pair.
- Switch configuration and statistics are synchronized between the primary and backup Extreme Campus Controller.
- RF Domain database is synchronized. RF Manager engines work from a synchronized database to preserve and respect AP SmartRF state on failover.
- Access points are *not* automatically upgraded. You must initiate the AP upgrade manually after both controllers in an Availability Pair are upgraded.

The following status data is replicated on the partner node of an Availability Pair:

- Client Records
- Group Records
- Registered Users and Devices

Related Topics

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 61).
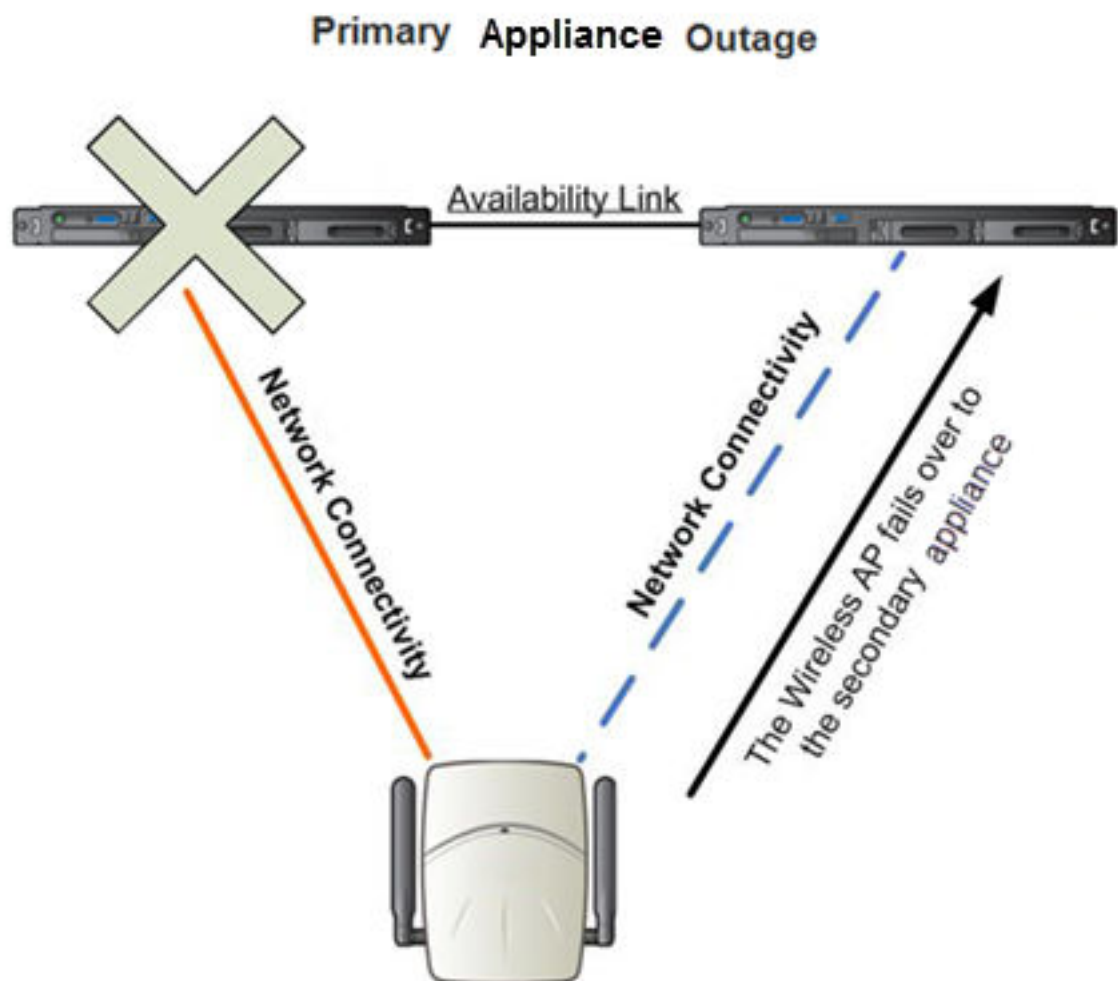
Figure 61: AP Fail Over When Primary Appliance Fails

- The wireless AP's network connectivity to the primary appliance fails (see Figure 62).
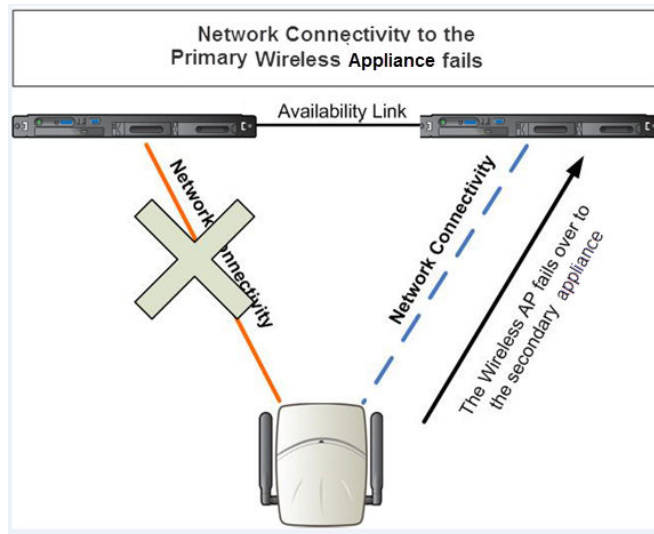
Figure 62: AP Fail Over When Connectivity to Primary Fails

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

In session availability mode (Figure 63), the APs connect to both the primary and backup Extreme Campus Controller. While the connectivity to the primary Extreme Campus Controller is via the active tunnel, the connectivity to the backup Extreme Campus Controller is via the backup tunnel.
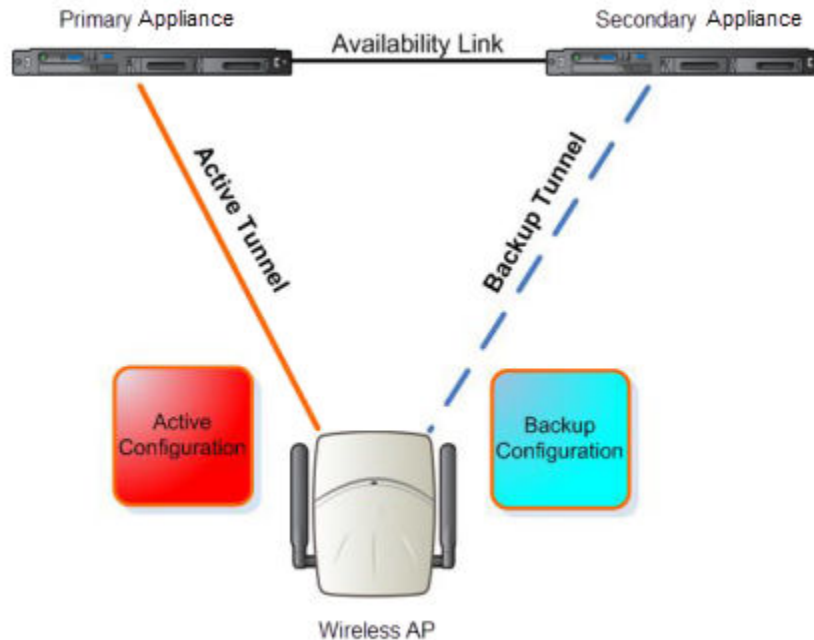
Figure 63: Session Availability Mode

The following is the traffic flow of the topology illustrated in Figure 63:

- The AP establishes the active tunnel to connect to the primary Extreme Campus Controller.
- The Extreme Campus Controller sends the configuration to the AP. This configuration also contains the port information of the backup Extreme Campus Controller.
- On the basis of the backup Extreme Campus Controller port information, the AP connects to the backup Extreme Campus Controller via the backup tunnel.
- After the connection is established via the backup tunnel, the backup Extreme Campus Controller sends the backup configuration to the wireless AP.
- The AP receives the backup configuration and stores it in its memory to use it for failing over to the backup Extreme Campus Controller. During this entire time, the AP is connected to the primary Extreme Campus Controller via the active tunnel.

Session availability applies only to the following topologies:

- Bridge Traffic Locally at AC
- Bridge Traffic Locally at AP

Availability Pair Settings

Table 89: 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 224

Mobility Settings

To configure Extreme Campus Controller as an agent in a mobility domain:

1. Go to **Admin** > **System** > **Availability**.
2. Check **Mobility** and configure the following parameters:

Table 90: Mobility Settings

Field	Description
Port	The port address of the Extreme Campus Controller.
Discovery Method	Method by which Extreme Campus Controller discovers the mobility manager. You have two options: • **SLPD** — Rely on SLP with DHCP Option 78 • **Static Address** — Define at the agent, the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended to provide tighter control of the registration steps for multi-domain installations.

Related Topics

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 Extreme Campus Controller settings from the **Admin** menu:

- SNMP
- MAC Format
- Cloud Visibility
- Tx Power Representation
- External NAT

Related Topics

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.

Extreme Campus Controller offers SNMP configuration for the full appliance or configuration for switches associated with a specific site.

To configure SNMP for the full Extreme Campus Controller environment:

Go to **Administration** > **System** > **Settings** > **SNMP**.

To configure SNMP for the switches associated with a site:

1. Go to **Configure** > **Sites** and select a site.
2. Select **Advanced**, and then select a value from the **SNMP** field.

Table 91 describes how to configure SNMP credentials on Extreme Campus Controller.

Table 91: 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 Extreme Campus Controller environment support only.
SNMPv3 Users	Select **Add** to add users for access to Extreme Campus Controller through SNMP. These values are typically types of users that are configured for access: • No Authentication/No Privacy • Authentication/No Privacy • Authentication/Privacy You can also edit user credentials and delete users.
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 Extreme Campus Controller environment support only.	
Context String (SNMPv3)	A description of the SNMP context. An SNMP context is information that you can access through the SNMP agent. A device can support multiple contexts.
Engine ID	The SNMPv3 engine ID for the appliance running the SNMP agent. The Engine ID must be from 5 to 32 characters long.
Forward Traps	Specify the level of the messages to be trapped. Valid values are: • None • Information • Minor • Major • Critical

Related Topics

Working with SNMPv2 Communities on page 314

Working with SNMPv3 Users on page 314

Working with SNMP Notifications on page 315

Settings on page 312

MAC Format on page 315

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 Extreme Campus Controller 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

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

MAC Format

Extreme Campus Controller provides the ability to define the user MAC address format for MAC-based authentication. Select from a set of MAC encoding formats, to match the format that you are using in your existing authentication infrastructure.

Select the MAC address format and click **Save**.

Related Topics

Enable Cloud Visibility

To enable Cloud Visibility:

1. Go to **Administration** > **System** > **Settings**.
2. Scroll down to the **Cloud Visibility** pane.
3. Select **Enable**.

The MAC address and serial number for the Extreme Campus Controller are displayed. These values are required as part of the onboarding registration of the appliance in ExtremeCloud IQ.

4. Provide the fully-qualified host name of the ExtremeCloud IQ server.

   This information is available from your ExtremeCloud IQ account. For example:

   `<RDC name>-cw.extremecloudiq.com` where:

   - `<RDC name>` is your Regional Data Center (RDC) information available under **About ExtremeCloud IQ**.
   - `-cw` indicates an Extreme Campus Controller appliance.
   - `.extremecloudiq.com` ExtremeCloud IQ host address.

5. Select **Save**.

> **Note**
> The reporting interval is 5 minutes.

Related Topics

Device Information Available in ExtremeCloud IQ

Extreme Campus Controller now integrates with ExtremeCloud IQ to manage access points and controllers from the cloud. This topic outlines the type of information available from ExtremeCloud IQ:

AP Device List

The following information is available in ExtremeCloud IQ from the Device List:
- Device Status (Online/Offline)
- Hostname
- Management IP address
- RF Domain Manager
- Cloud Config Group
- Serial Number
- Model Number
- Firmware Version
- Client Count
- Uptime

AP Overview Details

The following information is available for each device under **Monitoring** > **Overview**:
- Device Status (Online/Offline)
- Hostname
- Model
- CPU Usage
- Memory Usage
- Client Count
- SSID
- Tx/Rx

AP Wireless Interfaces Details

The following information is available for each device under **Monitoring** > **Wireless Interfaces**:

- Client Count
- Channel Utilization
- Channel Width
- Channel
- Neighboring APs

Clients List

The following information is available in ExtremeCloud IQ from the Clients List:

- Hostname
- Connection Status
- IP address
- MAC address
- VLAN
- SSID
- Last Session
- Time Connected to AP
- Channel
- Auth Method
- IPv6 address

Client Per Device Details

The following information is available for each client:

- Hostname
- IP address
- MAC address
- VLAN
- SSID
- Channel
- IPv6 address
- Connected to AP
- Average Received Signal Strength (RSSI)
- Average Signal to Noise Ratio (SNR)

AP Transmit Power Representation

You have the option to display AP power representation per chain or total power per radio for the ExtremeWireless 11ax access points.

The benefits of configuring power representation per chain, is to accommodate for different radio operation modes, including low power modes, which are smaller values than total radio power. Based on the AP Transmit Power Representation setting, the following AP related information is affected:

- Calculations and configuration related to the operational mode or antenna configuration.

- Displayed statistics and reported values from the AP to the appliance.

To configure the AP Transmit Power Representation:

1. Go to **Administration** > **System** > **Settings**.
2. Scroll down to the **AP Transmit Power Representation** pane.
3. For Configure and Report Tx Power, select **Per Chain** or **Total Per Radio**.
4. Select **Save**.

Related Topics

External NAT

Extreme Campus Controller supports External Network Address Translation (NAT), providing a secure means for remote users to access a campus network.

Configure a single address as an intermediary between the public internet and your private campus network. NAT improves network security by controlling access to the public network.

When deploying Extreme Campus Controller on private network behind NAT, configure the network as follows:

- Configure two external internet connections for High Availability and identify the IP address of each connection.
- On each Extreme Campus Controller, configure a physical or Bridged@AC VLAN with Device Registration enabled. The VLAN has an internal IP address.
- On each NAT device, configure a port mapping from external port 4500 to the IP address of Extreme Campus Controller (physical Bridged@AC VLAN, port 4500).
- On each Extreme Campus Controller, configure the external NAT IP address.

To configure the external NAT IP address on Extreme Campus Controller:

1. Go to **Administration** > **System** > **Settings**.
2. Scroll down to the **External NAT** pane.
3. Enter the IP address of the NAT device on the public internet.
4. Select **Save**.

This feature is supported in a High Availability Pair, but The External NAT IP address configuration is specific to each controller. The settings are not synchronized in a High Availability pair.

> **Note**
> The High Availability failover list is limited to a four IP addresses. The external IP address counts as one address in the failover list; therefore, only three topologies with device registration enabled are supported. If you have four VLANs with device registration enabled, Extreme Campus Controller will not configure the external NAT IP address. Similarly, when an external NAT IP address is configured, you cannot enable device registration on a fourth VLAN. The update will be refused.

All ExtremeWireless access points that are supported by Extreme Campus Controller support External NAT.

Related Topics

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 Extreme Campus Controller station events log.

Enable **Forward Station Events as Traps** to notify the administrator of events without solicitation. An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions. Traps can save network resources by reducing SNMP polling.

Syslog

Provide the IP Address of 1-3 syslog servers and enable the type of messages that you want to send to the syslog servers.

- **Send all Service Messages**
- **Send Audit Messages**
- **Send Station Events**

> **Note**
> To synchronize the logs, the syslog daemon must be running on both the appliance and on the remote syslog server. When you change the log level on the appliance, you must modify the appropriate setting in the syslog configuration on remote syslog server.

Facility Codes

Facilities codes identify log streams in the remote syslog server. Select a unique facility code (local.0 - local.6) for each Extreme Campus Controller facility to differentiate the log streams and facilitate the filtering of messages.

The facility code applies to all three servers. Select a facility code for each of the following:

- Application Facility
- Service Facility
- Audit Facility
- Station Facility

Related Topics

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 64: Example System Information

```
Manufacturing Information

SMX Version: 04.26.01.0160
GUI Version: 04.26.01.0160
NAC Version: 8.1.52.26
Software Version: 04.26.01.0160T
Model: VE6120 Small
CPU Type: Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz
CPU Frequency (MHz): 2093.962
Number of CPUs: 4
Total Memory: 8172184 KB
HW Encryption Support: Yes
LAN 1  MAC address: 00:50:56:AB:1B:AD
LAN 2  MAC address: 00:50:56:AB:49:B5
ADMIN  MAC address: 00:50:56:AB:D1:0D
```

Figure 65: Example Manufacturing Information

Manage Administrator Accounts

Extreme Campus Controller is shipped with a factory-set, default administrator account with full rights:

- The user ID is `admin`.
- The factory preset password for this account is `abc123`.

These values are case sensitive. During initial configuration of Extreme Campus Controller, the CLI wizard prompts you to change the default Admin user ID and password.

To add administrator accounts:

1. Go to **Administration** > **Accounts**.
2. Select **Add** and configure the following parameters:

   Username

   User name for the administrator account.

   Password

   Password for the administrator account.

   Confirm Password

   Re-enter password for the administrator account.

   Admin Role

   Select the level of access privileges for the administrator account. Valid values are:

   - Full. Full administrative privileges.
   - Read-Only. Ability to log on and view administrative pages.
   - Custom. Configure user access to specific areas and features of Extreme Campus Controller. Select **Custom** > **Configure** to display the list of Admin roles.

3. To edit account settings:

   a. Select and existing account from the list.

   b. Modify settings as necessary, and select **Save**.

   > **Note**
   > You can generate API keys that are used to access Extreme Defender Application when editing an existing user account.

4. To delete an existing account:

   a. Select and existing account from the list.

   b. Click **Delete**.

   > **Note**
   > All administrator accounts *except* the default account can be deleted.

Related Topics

Manage RADIUS Servers for User Authentication

Configure a list of RADIUS servers to authenticate users of Extreme Campus Controller.

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 Extreme Campus Controller. 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

Custom User Account Access

You can configure separate user access to specific areas and features of Extreme Campus Controller.

1. Go to **Administration** > **Accounts**.
2. To display account parameters, select an account or select **Add**.
3. From the **Admin Role** field, select **Custom** > **Configure**.
4. Select **Read-Only** or **Read-Write** for each of the following product areas.

Read-Only access enables you to view or monitor the area. **Read-Write** access enables you to configure the area.

> **Note**
> When configuring a new account, you have the option to configure a **Preset** access level that applies to all areas of Extreme Campus Controller.

Site

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

- Sites on page 91
- Sites List on page 37
- Configuring Roles on page 213
- Configuring VLANS on page 224
- Configure a Mesh Point Network on page 188
- Configuring a Floor Plan on page 138
- AAA RADIUS Authentication on page 242
- Clients on page 79

Networks

Monitor or configure Extreme Campus Controller networks. See Managing a Network Service on page 212 and Networks List on page 76.

Access Points

Monitor or configure Extreme Campus Controller access points. See Access Points on page 148 and Access Points List on page 50.

Switches

Monitor or configure Extreme Campus Controller switches. See Switches on page 170 and Switches List on page 72.

eGuest

Monitor or configure Extreme Campus Controller integration with ExtremeGuest. See ExtremeGuest Integration on page 240.

Adoption

Monitor or configure Extreme Campus Controller Adoption rules. See Automatic Adoption on page 233.

Troubleshoot

Monitor or configure packet capture for sites and device groups and open a remote console. See Packet Capture on page 64 and Opening Live SSH Console to a Selected AP on page 68.

Onboard AAA

Monitor or configure AAA policy and add Local Accounts. See Onboard AAA Authentication on page 247.

Onboard Captive Portal

Monitor or configure Extreme Campus Controller internal captive portal. See Managing Captive Portal on page 257.

Onboard Groups and Rules

Monitor or configure access control groups and rules. See Managing Access Control Groups on page 269 and Access Control Rules on page 272.

Onboard Guest CP

Monitor or configure Extreme Campus Controller ExtremeGuest captive portal settings. See ExtremeGuest Captive Portal Settings on page 207.

Platform

Monitor or configure Administration system settings. See System Configuration on page 295.

Accounts

Monitor or configure Administration account settings. See Manage Administrator Accounts on page 321.

Applications

Monitor or install and configure Docker applications. See Extreme Campus Controller Applications on page 324.

Licensing

Monitor or configure Administration Licensing. See Product License on page 335.

CLI Access

Access to the Switch CLI Console. See Access the Switch CLI on page 177.

Related Topics

Manage Administrator Accounts on page 321

Extreme Campus Controller Applications

Extreme Campus Controller operates as the base operating system for container applications that will share its resources.

Extreme Campus Controller supports container applications that offer custom solutions for network management. Applications are installed as .Docker files available on Extreme Networks support site or downloaded from the Docker hub.

> **Note**
>
> You can install the application from a local image file or you can download an image file from Docker Hub. Before an image file is downloaded from Docker Hub, Extreme Campus Controller checks the image version. When a newer version is available, a message is displayed on the Extreme Campus Controller user interface. Extreme Campus Controller does not download information from Docker Hub. It only checks the application version.
>
> Extreme Campus Controller supports integration with Amazon Greengrass. Therefore, it periodically checks availability of the service. Extreme Campus Controller does not upload or download information to and from these services.
>
> Communication from Extreme Campus Controller to Docker Hub or AWS can be blocked on the firewall. When communication is blocked, the application continues to operate normally, but you will not be notified when a newer image file is available on Docker Hub.

> **Note**
>
> A Domain Name Server (DNS) is required when deploying container applications because the application logic may require access to external resources (such as the Docker Repository). For information about configuring a Domain Name Server (DNS), see the Extreme Campus Controller Deployment Guide.

Related Topics

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 Extreme Campus Controller
> - AirDefense Base Application

For more information about template configuration settings, see Configuration Template Details on page 327.

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 333.

> **Note**
>
> Extreme Campus Controller supports installation of a Docker file with a specific numerical version. Applications indicating the *"Latest Version"* or version numbers that include alphabetic characters are not supported. Twenty percent of the appliance hardware capacity is allocated for Docker file applications.

Take the following steps to install an application:

1. Go to **Administration** > **Applications**.
2. Select **Add** to create the Configuration Template.

> **Note**
>
> Several Extreme applications include default templates that cannot be edited. Skip this step when installing:
> - Extreme Defender Application
> - Scheduler for Extreme Campus Controller
> - AirDefense Base Application

3. Select ⊕ to add an application to Extreme Campus Controller.
4. Install from a local **File** or Docker hub **Registry**.
5. To install directly from the Docker hub, select **Registry**, then **OK**. Or,
6. To install a local file, select **File** > **Upload**.
7. Navigate to the Docker file and select **Open**.
8. Select **OK**.

   The application is uploaded and installed on Extreme Campus Controller.
9. Generate an API key and associate it with the application before running the application.

Select ▶ to start the application.

> **Note**
>
> You must generate an API Key and associate it with the application before running the application.

The following describes the available application actions:
- ⊕ — Install new application.
- ✎ — Edit Configuration Template. (Not available for Extreme Defender Application or Scheduler for Extreme Campus Controller.)
- ⬆ — Upgrade existing application.
- ⊖ — Uninstall application.
- ▶ — Start application.
- ⬛ — Stop application.
- ⊙ — Show application statistics. Displays dashboard widgets, configuration details, and logs, and it provides console access to the application for troubleshooting.

Related Topics

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 Extreme Campus Controller
> - AirDefense Base Application

Use a configuration template to install and upgrade container applications in Extreme Campus Controller.

To add a template:

1. Go to **Administration** > **Applications** and select **Add**.
2. Configure the following parameters:

Table 92: 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 Extreme Campus Controller. • The internal port in the container must be TCP port 8887. • The base URL must begin with the application name. For example: /defender. • The application must use relative URLs.
Icon	The application icon. Select **Change** to select a new image file. After selecting a new image file, the **Default** button displays. Select **Default** to revert to the default image.

Table 92: Container Application Configuration Template (continued)

Field	Description
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 Extreme Campus Controller. • syslog. View application logs from the System log file. • gelf. Graylog Extended Log Format.
Restart Policy	Indicates the application restart behavior when Extreme Campus Controller is started. Valid values are: • Always. The application will always restart. • Unless Stopped. The application will restart unless it was manually stopped prior to the Extreme Campus Controller start. The application will keep its current state. • Failed. Will restart only after an application failure.
CPU Limit	Used to manage CPU allocation when multiple applications are installed. Max limits are dependent on the appliance platform limitations.
Memory Limit (MB)	Used to manage memory allocation when multiple applications are installed. Max limits are dependent on the appliance platform limitations. Default value is 50 percent of maximum limitation.
Volume Mapping	Indicates folder name and path for volume storage. Volume storage will not be deleted upon application *upgrade*. **Note:** All data is deleted when the application is *uninstalled*.
Config Files Mapping	Indicates folder name and path for configuration files, including API key files.
Port Mapping	Configure source and destination ports for the application. The external port range must be 32768-65535, because this is the open port filter range.
Environment Variables	Configure environment variables.

Related Topics

Access an Application

After an application is installed on Extreme Campus Controller, take the following steps to access the application:

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

    The applications that Extreme Campus Controller supports by default are listed. Applications that are installed and running are indicated by a green dot icon.

2. To open an application in a separate browser window, select the application.

3. Alternately, you can access an application user interface using the HTTPS protocol on the TCP port 5825. For example, if your Extreme Campus Controller has the IP address 192.168.10.10, you can manage the container application in a browser by typing `https://192.168.10.10:5825/apps/[application_name]` into the URL field.

Table 93: Application Names in Browser Address

Application	Application in browser address
Extreme Defender Application	`apps/defender`
AirDefense Base	`apps/airdefense_base`
Scheduler for ExtremeCloud Appliance	`apps/extreme-scheduler`

The login screen for the selected application displays. Your login credentials will match your Extreme Campus Controller 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. SA201 supports enforcement for up to eight end-systems, connected through the wired client port.

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

Extreme Campus Controller offers a default configuration template for the Extreme Defender Application. This template cannot be modified.

> **Note**
> The Extreme Defender Application is available on the Extreme Networks support site.

To install Extreme Defender Application:

1. Download and install the Docker application.
2. Generate the API key.
3. Associate the API key with the Docker application.

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

4. Start the application.

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

Additionally, the Extreme Defender Application user interface can be accessed using the HTTPS protocol on the TCP port 5825. For example, if your Extreme Campus Controller has the IP address 192.168.10.10, you can manage Extreme Defender Application in a browser by typing `https://192.168.10.10:5825/apps/defender` into the URL field.

Related Topics

Scheduler for Extreme Campus Controller

Schedule network services with the latest Docker application Scheduler for Extreme Campus Controller.

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

Extreme Campus Controller offers a default configuration template for Scheduler application. This template cannot be modified.

> **Note**
> Scheduler for Extreme Campus Controller is available on the Extreme Networks Support site.

To install Scheduler for Extreme Campus Controller:

1. Download and install the Docker application.
2. Generate the API key.
3. Associate the API key with the Docker application.

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

4. Start the application.

Related Topics

Generate API Keys on page 333

REST API Access for Docker Container Applications on page 333

Install an Application on page 325

Associate API Key File with a Docker Application on page 335

Upgrade an Application on page 329

Uninstall an Application on page 330

Application Details on page 330

AirDefense Base Application

The AirDefense Base Application offers a free Wireless Intrusion Prevention System (WIPS), enabling you to configure a port for WIPS.

The AirDefense Base Application is installed as a container application on Extreme Campus Controller. The application runs and is upgraded independently from the appliance. After you install and start the AirDefense Base Application, it listens to the AP connections and interacts with Extreme Campus Controller to gather the status of the AP.

You must configure an ADSP configuration Profile to work with AirDefense Base Application. For more information, see AirDefense Profile Settings on page 113.

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

Related Topics

AirDefense Profile Settings on page 113

REST API Access for Docker Container Applications

Use an API key to allow Docker containers access to the Extreme Campus Controller REST API. A randomly generated key allows access to Extreme Campus Controller without requiring the user to be actively logged in, and it can allow access privileges that are greater than the privileges of the application user. The API key can be used in place of the password of the original account.

> **Note**
> When running more than one Extreme Campus Controller 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

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

1. Go to **Administration** > **Accounts**.
2. Select a user account.

3. From the API Keys field, select **Generate New API Key**.

   The key is generated. The **API Key** dialog displays.

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.
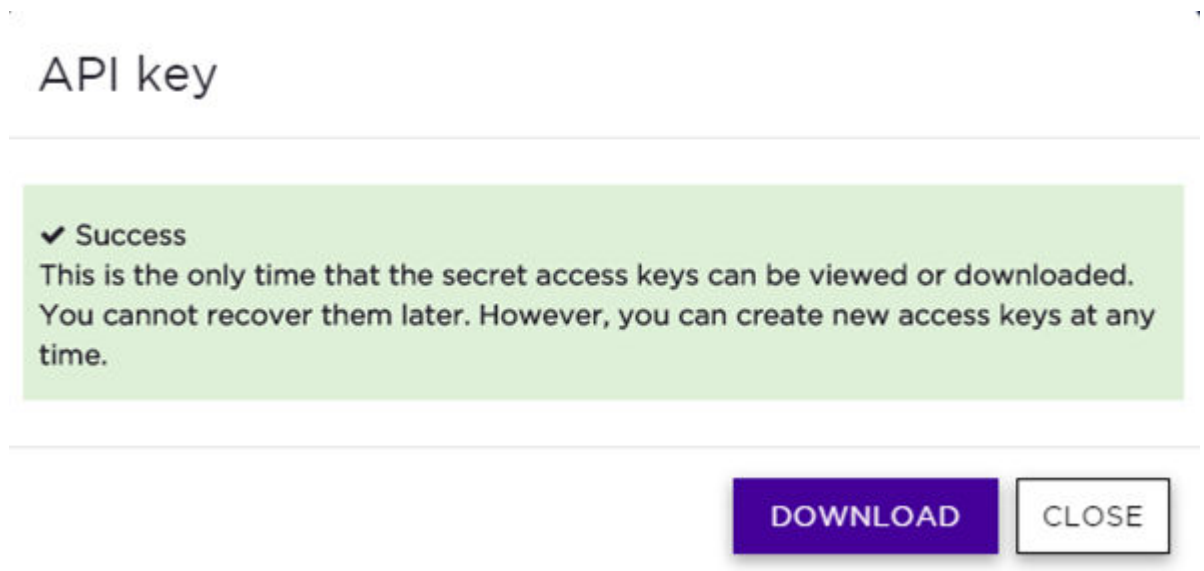
DOWNLOAD   CLOSE

Figure 66: API Key dialog

4. To download the API key as a .json file, select **Download**.

   Download the key immediately. If you select **Close**, you will not be able to access the key. You can generate additional keys at any time.

5. After you download the key, select **Close**.

Related Topics

> Delete API Keys on page 334
> REST API Access for Docker Container Applications on page 333
> Associate API Key File with a Docker Application on page 335
> Configuration Template Details on page 327
> Manage Administrator Accounts on page 321

Delete API Keys

Generated API keys are listed on the user account page. To delete a key:

1. Go to **Administration** > **Accounts**..
2. Select a user account.
3. Select a key from the API Keys list, and select 🗑.

   A verification message displays.
4. To delete the API key file, click **OK**.

Related Topics

> Generate API Keys on page 333

Associate API Key File with a Docker Application

To upload a generated API key file:

1. Go to **Administration** > **Applications** and select ◙.
2. Select the **Configuration Files** tab.
3. Select **api-keys.json**, and then select the upload icon ⬆ .
4. Upload the API key file one of the following ways:

    - Click the **Choose File** box and navigate to the downloaded API key file.
    - Drag and drop the downloaded API key file onto the **Choose File** box.

    The API key file displays in the **Configuration Files** list.

Related Topics

Generate API Keys on page 333

Remove a Configuration File from a Docker Application

Take the following steps to remove a configuration file from a Docker application:

1. Go to **Administration** > **Applications** and select ◙.
2. Select the **Configuration Files** tab.
3. Select a configuration file, then select 🗑.

    A verification message displays.
4. To remove the configuration file, select **OK**.

Related Topics

Associate API Key File with a Docker Application on page 335
Configuration Template Details on page 327
Manage Administrator Accounts on page 321
Generate API Keys on page 333
Delete API Keys on page 334

Product License

To license Extreme Campus Controller your first step is to go to the support portal and generate the Activation Package. For every Extreme Campus Controller instance, you are required to complete a one-time-only activation process for each instance of Extreme Campus Controller. The activation process is required for all Extreme Campus Controller installations.

➡ **Important**
Ensure that Extreme Campus Controller is configured with the correct Network Time Protocol (NTP) Server settings. Licensing management and several other system functions are dependent on an accurate timestamp. Configure NTP settings on Extreme Campus Controller during the initial setup wizard or alternatively under **Administration** > **System** > **Network Time** (as a first configuration step).

The following Activation types are available:

- **Evaluation** — (Temporary) A temporary activation comes with a regulatory domain. With the temporary activation, you can select a country from the domain and operate the APs on any channel

permitted by the country. A temporary activation 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 is valid for 90 days. Once the 90-day period is up, the temporary activation expires. You must get a permanent activation and install it on the appliance. Extreme Campus Controller will warn you to obtain a permanent license seven days before the expiration date. If you do not install an activation package, the appliance generates event logs every 15 minutes, indicating that an appropriate license is required for the current software version. In addition, you will not be able to edit the Network Service parameters.

- **Permanent** — A permanent activation is valid for the contractual period.

Each Extreme Campus Controller 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 an EGY license can manage access points deployed in Egypt.

> **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.

You have the option to license your Extreme Campus Controller through subscription or through a permanent capacity key. Regardless of the licensing model you choose, you must generate and install an Activation Package for each instance of Extreme Campus Controller.

Related Topics

Licensed Devices

Extreme Campus Controller supports the following access point models:

- AP310i/e
- AP360i/e
- AP410i/e
- AP460i/e
- AP505i

- AP510i/e
- AP560i/h

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

The access points are manufactured with a specific domain lock. They are configured for either an FCC or ROW license domain.

For a list of supported switches, see the *Release Notes*.

Related Topics

Product License on page 335

Generate and Install the Activation Package

All customers must generate and install an Activation Package for Extreme Campus Controller. Regardless of whether you obtain a new license or upgrade to Extreme Campus Controller. Take the following steps to generate and install the Activation Package:

1. Log in to Extreme Campus Controller
2. Go to **Administration** > **License** to obtain the system **Locking ID**.
3. Log into the Extreme Support Portal: https://extremeportal.force.com/ExtrSupportHome.
4. Go to **Assets** > **Licenses Home** and select the Extreme Campus Controller Voucher ID line item from the list.
5. On the **Voucher Details** page, select **Generate Activation Key**.
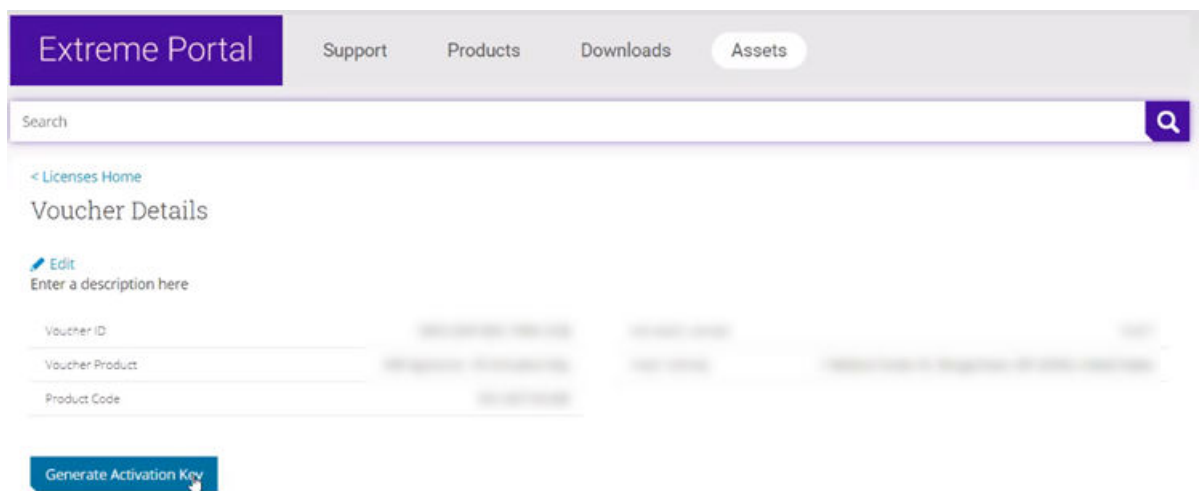
Figure 67: Generate Activation Key

6. Provide the Locking ID for the Extreme Campus Controller that will be activated.

7. Check the box to accept **Terms and Conditions** and select **Submit**.
8. The Activation package is generated, and the **Save As** dialogue displays.
9. Download the Activation Package to your local machine.

> **Note**
> The Activation Package *file name* includes the Locking ID for the specific Extreme Campus Controller.

Install the Activation Package

Stage your Extreme Campus Controller instance. Install the Activation Package to activate Extreme Campus Controller:

1. Return to the Extreme Campus Controller instance from where you obtained the Locking ID.
2. Go to **Administration** > **License**.
3. Select the plus sign next to the **Activation License** field.
4. Drag the Activation Package to the **Upload License** dialog to install the Activation Package.

Related Topics

Subscription License

Subscription licensing is available for Extreme Campus Controller for both access point and switch management. Upon purchase of a new Extreme Campus Controller you will receive a welcome email and activation instructions.

Each appliance obtains capacity Right to Use (RTU) entitlements regarding managed devices, subject to the system limits of the appliance instance and the total number of activations purchased. The total consumed RTU across all Extreme Campus Controller instances cannot exceed the number of RTU you have subscribed to. Each appliance provides visualization on specific RTU allocation and overall balance. For subscription management, Extreme Campus Controller requires a configured DNS server and constant connection to the Internet in order to be operational.

Related Topics

Licensing States

Without a valid license applied, Extreme Campus Controller presents the following states:

- 7-day Activation Period — Extreme Campus Controller gives you seven days to apply a valid Activation Package. A banner indicates the number of days you have remaining in this state.
- License Violation / Lockdown — On day 8, if you have not applied a valid license, your appliance will enter License Violation state. In this state, Extreme Campus Controller is in a read-only mode, only the License Page is read-write, allowing you to install a valid Activation Package. Critical logs are generated every hour. This state lasts for seven more days.

For a subscription license only, Extreme Campus Controller connects once each day with the licensing server. When necessary, you can manually synchronize Extreme Campus Controller with the licensing server. You may want to manually synchronize after the following conditions:

- A change in capacity entitlements
- After applying a valid license
- After a failover in an Availability Pair.

To manually synchronize:

1. Go to **Administration** > **License** > **License Details**.
2. Select **Synchronize Now**.

> **Note**
> Connection Issue (Subscription Licensing Only) — In the event that the Extreme Campus Controller cannot connect to the licensing server after you have installed and Activation Package for a subscription license, Extreme Campus Controller gives you three days to rectify the connection issue. If the controller cannot reach the licensing server in three days, on the fourth day, the controller goes into a Violation State for seven days. If the connection to the licensing server cannot be restored within the full 10-day period, the controller goes into Lockdown state.

Related Topics

Generate and Install the Activation Package on page 337

Licensing an Availability Pair

In an Availability Pair, Right to Use (RTU) for APs and switches are shared in a common pool by both primary and backup controllers. When both Extreme Campus Controller are operational and the tunnel is up, the primary controller checks the licensing server for APs on the both controllers. When the primary Extreme Campus Controller is down, the backup controller checks with the licensing server for APs. The backup controller will be synchronized upon the next automatic sync with the licensing server. You can also manually sync with the licensing server. Select **Synchronize Now**.

> **Note**
> The Deployment ID for controllers in a High Availability pair is the Locking ID of the primary Extreme Campus Controller.

Permanent Capacity License

A Permanent Capacity License is a one-time license that allows permanent activation, and it works with a separate Capacity key. The alternative to a Permanent Capacity License is a Subscription License. The activation process is the same regardless of the license model you choose.

The Extreme Campus Controller permanent capacity 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 enhance the capacity of the controller to manage additional APs.

> **Note**
> The controller does not require internet access with Permanent Capacity Licensing.

- Capacity key — Enhances the capacity of the appliance to manage devices. Extreme Campus Controller supports capacity enhancement keys for 5, 25, 100, 500 or 2000 APs. Max capacity on an Extreme Campus Controller instance is subject to the appliance type and the capacity tier configured (based on hypervisor resources for Virtual instances).

  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. Extreme Campus Controller 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 Extreme Campus Controller if its peer has the same capacity key applied.

To obtain a Permanent Capacity License:

1. Go to the Support portal to generate an Activation Package. For more information, see Generate and Install the Activation Package on page 337.
2. From the Support portal, obtain your capacity keys. For more information, see Obtain an Apply a Capacity Key on page 341.

   There is no connection to the licensing server when an Activation Package for Permanent Capacity Licensing is installed. Therefore, the Extreme Campus Controller displays a connection failure message. This message can be ignored for Permanent Capacity Licensing. Simply select the **Switch to Permanent Licensing** link to clear the message.
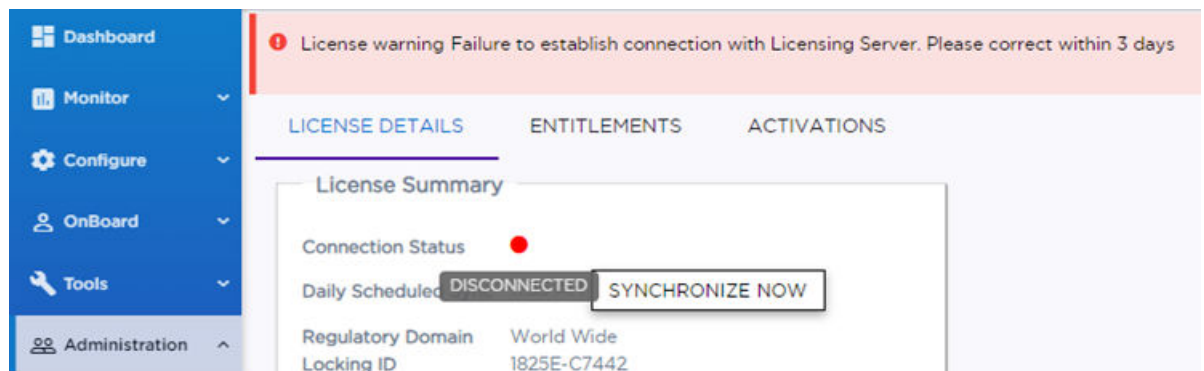
Figure 68: Connection to License Server message when Permanent Licensing is applied

3. After selecting **Switch to Permanent Licensing**, your valid capacity limits are displayed.
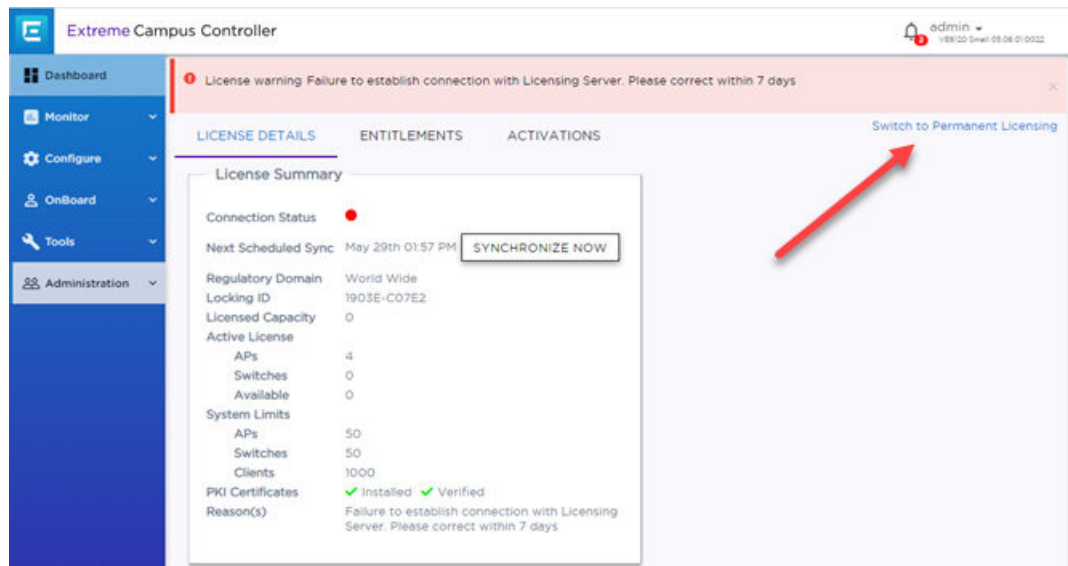
Figure 69: Switch to Permanent Capacity Licensing

Related Topics

Obtain an Apply a Capacity Key

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

   The Extreme Networks Support portal presents the Capacity key.
3. On the Extreme Campus Controller, go to **Admin** > **License**.
4. Select the **Permanent Capacity License** link.
5. Next to the **Licensed Capacity** field, select the plus sign.
6. Copy and paste the Capacity key from the Extreme Networks Support portal to the Extreme Campus Controller user interface.
7. Select **Apply**.

> **Note**
> When using a Permanent Capacity License model, on Extreme Campus Controller, select the **Permanent Capacity License** link. Your valid capacity limits are now displayed.

Upgrade to Extreme Campus Controller

All customers who are upgrading to Extreme Campus Controller must obtain a new Activation Key.

> 📝 **Note**
> Upgrading from v4.76.x to v5.06.x will result in a license violation. You must apply a new Activation Package for Extreme Campus Controller.

1. Log into the Extreme Support Portal: https://extremeportal.force.com/.
   For more information, refer to *Extreme Campus Controller Upgrade Service Contract*.
2. Generate a new Activation Package and install it on the appliance. For more information, refer to Generate and Install the Activation Package on page 337.

> 📝 **Note**
> For every Extreme Campus Controller instance, you are required to complete a one-time-only activation process for each instance of Extreme Campus Controller. The activation process is required for all Extreme Campus Controller installations.

The Activation Package includes your Customer Unique ID (CUID), capacity limits, and certificates for a virtual appliance. (Physical appliances include certificates pre-installed.) You are ready to start managing devices with Extreme Campus Controller.

When using a Permanent Capacity License model, select the **Permanent Capacity License** link. Your valid capacity limits are now displayed.

Related Topics

Entitlements

The Extreme Campus Controller **Entitlements** page is a log of all purchased entitlements associated with the customer account. Purchase the entitlements using a Capacity key. Entitlements indicate the total number of devices you are licensed to manage per your customer account. Each entitlement has a Start and End date.

To view the list of entitlements, go to **Administration** > **License** > **Entitlements**.

Figure 70: License Entitlements

Related Topics

Activations

The Extreme Campus Controller **Activations** page displays a view of activations. Activations indicate the number of devices the specific appliance is actively managing. Each licensed activation has a Start and End date.

To view the list of activations, go to **Administration** > **License** > **Activations**.
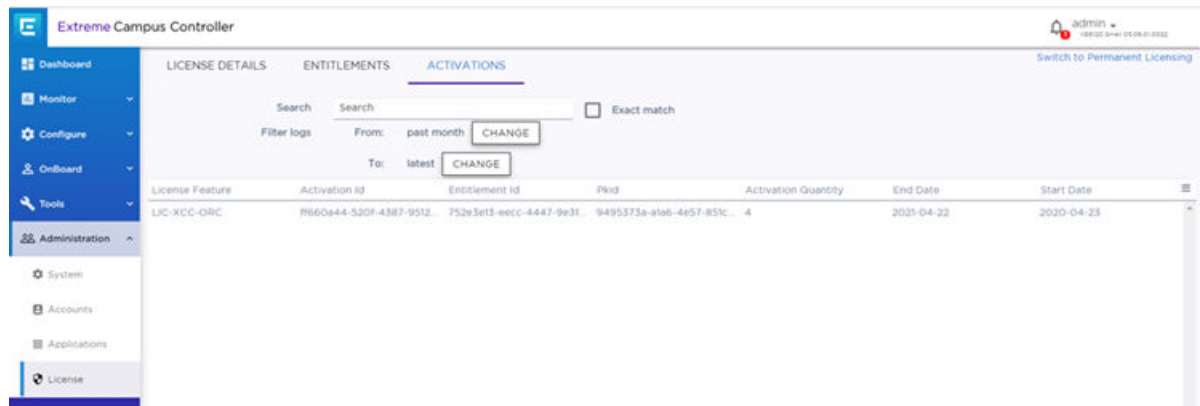
Figure 71: License Activations

Related Topics

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 Campus Controller

ExtremeCloud Appliance has been rebranded to Extreme Campus Controller. The new Extreme Campus Controller supports Campus/Centralized sites only. Support for Distributed sites remains in ExtremeCloud Appliance v4.76.02 and later.

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

The Extreme Campus Controller includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge.

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. Extreme Campus Controller™ 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 (), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. 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, becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about 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

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/support/documentation/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 Wi-Fi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

Index

C

D

E

F

G

H