

ExtremeCloud Information Center

For Version 4.51.02



Copyright © 2019 Extreme Networks, Inc. All rights reserved.

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, please 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:

www.extremenetworks.com/support/policies/software-licensing

Table of Contents

Preface	6
Text Conventions.....	6
Providing Feedback to Us.....	6
Getting Help.....	7
Documentation and Training.....	8
Chapter 1: Azara Customer Assistance	9
Azara User Interface Mapping to ExtremeCloud.....	9
Azara FAQs and End of Service.....	10
Chapter 2: Product and Architecture Overview	11
Architecture.....	11
Topology.....	12
Access Points.....	14
ExtremeXOS Switches.....	14
Extended Edge Switches.....	16
NAT Branching.....	20
Site Management Protocol.....	20
Multiple Site Support.....	21
Authentication.....	22
Layer 7 Application Control.....	24
Statistics and Reporting.....	26
Extreme AirDefense Integration.....	26
ExtremeLocation Integration.....	26
Chapter 3: Connecting Your Devices to ExtremeCloud	28
Prerequisites to Deployment.....	28
System Limits.....	31
ExtremeCloud License Expiration.....	32
Create or Update Your Account.....	32
Use the Deployment Prerequisite Tool.....	32
Device Adoption Rules.....	34
Connect Switches.....	34
Connect Access Points.....	36
Chapter 4: Licensing and RMAs	39
10 Gbps Licensing for Switches.....	39
ExtremeCloud License Expiration.....	39
RMA Replacement Process.....	40
Chapter 5: User Interface	42
User Interface Details.....	42
User Interface Changes.....	43
Chapter 6: Dashboard	45
Statistics and Intervals.....	48
Configure the Dashboards.....	48
Chapter 7: Monitoring	51
Logging.....	51

Use Topology Manager.....	54
Monitor Sites.....	57
Monitor Networks.....	59
Monitor Access Points.....	60
Monitor Switches.....	62
Monitor Clients.....	64
Monitor Roles.....	67
Monitor Applications.....	68
Monitor Unsanctioned APs for ExtremeWireless WiNG.....	69
Chapter 8: How to Configure Your Network.....	71
Chapter 9: Configuring Sites.....	72
Configure a Site.....	73
Clone a Site.....	105
Delete a Site.....	106
System Log Configuration.....	106
How to Enable Location Analytics.....	106
SNMP.....	107
Wireless Intrusion Detection Services (WIDS).....	107
Chapter 10: Configuring Networks.....	109
Configure Network Services.....	110
Configure Advanced Network Settings.....	116
Chapter 11: Configuring Access Points.....	120
Dynamic Radio Management.....	121
Radios as Sensors.....	122
Configure ExtremeWireless Access Points.....	122
Configure ExtremeWireless WiNG Access Points.....	126
Configure Advanced Settings for an Access Point.....	129
Configure AP510e Professional Install Settings.....	134
Configure Advanced Radio Settings for AP5XX.....	135
Start Live Capture.....	137
Reboot an Access Point.....	137
Retrieve AP Trace Files.....	138
Upgrade AP3916ic.....	138
Chapter 12: Configuring Switches.....	140
LLDP Mode.....	141
Multiple Spanning Tree Protocol.....	141
Configure a Switch.....	142
View the PoE Budget.....	145
LAG Ports.....	146
MLAG.....	148
Configure an Individual Port.....	152
CLI Mode.....	156
Chapter 13: Configuring Policy.....	161
Roles.....	161
Network Policy Rules.....	163
Application Policies and Application Rules.....	168
Class of Service and ToS/DSCP.....	174

Tagged and Untagged VLANs.....	177
Configure Rates.....	181
How to Configure a Captive Portal.....	182
How to Limit Bandwidth.....	201
Chapter 14: Tools.....	202
Port Manager Overview.....	202
Use Packet Capture.....	205
Use Ping and Trace Route.....	207
Use the Wireless Debug Tool.....	208
Chapter 15: Reports.....	210
Create Templates and Run Reports.....	211
Run PCI Compliance Reports.....	213
Run Security Reports.....	216
View Scheduled Reports.....	219
View Generated Reports.....	219
View Audit Log Files.....	220
Chapter 16: Administration.....	221
Create, Modify, or Disable Administrator Accounts.....	221
Delete Administrator Accounts.....	224
Configure General System Settings.....	224
Configure Email Notifications.....	227
Assign Switch Licenses.....	228
Chapter 17: Troubleshooting.....	229
Understanding LED Patterns for AP Registration.....	229
Reset a Port.....	230
AP Not Connecting With Cloud.....	232
Chapter 18: REST API Software Development Kit (SDK).....	234
Log in to the REST API Server.....	234
Access the Documentation User Interface.....	236
Tools and Methods.....	237
Headers.....	238
Create a Basic REST API Command.....	238
MSP Examples.....	239
Network Management Examples.....	255
Glossary.....	289

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons





Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
<i>New!</i>	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

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

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have 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 especially want to know about:

- Content errors or confusing or conflicting information.

- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Please 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: 1-800-998-2408 (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 and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

Subscribing 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 with your information (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 Click **Submit**.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

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

1 Azara Customer Assistance

Azara User Interface Mapping to ExtremeCloud Azara FAQs and End of Service

Azara User Interface Mapping to ExtremeCloud

If you are a former Azara customer, the following table can help you learn how to access the equivalent Azara functionality in **ExtremeCloud**.

Table 3: Mapping Functionality Between Azara and ExtremeCloud

Azara Functionality	ExtremeCloud Functionality
Map view	Monitor Sites on page 57
System	<ul style="list-style-type: none">• Dashboard• <i>System</i> in Azara represents the tenant as a whole. The main dashboard lets you view comparable information for the tenant.
Custom dashboards	Configure the Dashboards on page 48
Monitor > Summary	Dashboard
Monitor > Access Points	Monitor > Devices > Access Points
Monitor > Clients	Monitor > Clients
Monitor > Event Log	Logging on page 51
Reports	Select Reports > Reports to access PCI Compliance and Security reports.
Configuration > Networks	<ul style="list-style-type: none">• Configure > Networks• Access points are automatically added to the AP list when they are registered using the process in your Welcome email
Configuration > Sites	Configure > Sites
Configuration > Captive Portal	Configure > Policy > Captive Portal
Configuration > Inventory/Devices	Configure > Devices > Access Points
Configuration > Users	Administration > Accounts
Configuration > Preferences	<ul style="list-style-type: none">• Most preferences are managed by selecting Configure > General• SNMP settings are set at the site level
Configuration > Licenses	Configure > Licenses

Azara FAQs and End of Service

If you are a former Azara customer, here are links to additional information to help in transitioning to ExtremeCloud:

- [Frequently Asked Questions](#)
- [End of Sale/End of Support Information](#)

2 Product and Architecture Overview

Architecture
Topology
Access Points
ExtremeXOS Switches
Extended Edge Switches
NAT Branching
Site Management Protocol
Multiple Site Support
Authentication
Layer 7 Application Control
Statistics and Reporting
Extreme AirDefense Integration
ExtremeLocation Integration

With zero-touch provisioning, ExtremeCloud simplifies the deployment, configuration and monitoring of access points (APs) and switches in your network infrastructure using a centralized management user interface. Supported device models are pre-provisioned from the factory to discover the ExtremeCloud solution set. An entitlement is required to use the ExtremeCloud management features.

This product:

- Provides automatic discovery and connectivity
- Does not require the deployment of a wireless LAN controller
- Does not require special firewall configuration
- Lets you configure and manage APs and switches (use of switches is optional)
- Provides reporting views showing the overall health of your network
- Lets you drill down to device-level reports to help you proactively plan or troubleshoot an issue
- Provides a programmable RESTful API

The first administrator account created has full privileges, and can create additional administrator accounts with full or read-only privileges.

More Information

- [Architecture](#) on page 11

Architecture

ExtremeCloud supports a variety of deployment models, from the simple deployment of one or more cloud-enabled access points (APs) to more complex deployments involving cloud-enabled switches. Cloud-enabled APs and cloud-enabled switches can be deployed with existing on-premise equipment.

The following sections explain the architectural components of the ExtremeCloud solution and illustrate some of the possible deployment scenarios.

Topology

The equipment that can participate with this product is pre-provisioned from the factory to directly connect to ExtremeCloud. No provisioning of your local infrastructure is required.

The network requirements are:

- You must have Internet access and have a DHCP server that provides cloud-enabled switches and APs with IP addresses and the address of a DNS server.
- Verify that Network Time Protocol (NTP) is allowed out through your firewall on port 123 so that the APs can submit NTP queries to pool.ntp.org to set their clocks.
- Each site must have L2 connectivity. The APs within a site operate within a single RF domain and therefore must have L2 connectivity to function properly.
- The best practice is to use a single VLAN for all the APs in a site instead of distributing the site's APs over multiple VLANs. If you decide to distribute a site's APs over multiple VLANs, then you must allow either routing or forwarding of SIAPP multicast between those VLANs.

The supported APs and switches provide automatic discovery using the standard HTTPS/SSL port number 443 that is allowed by most firewalls. Additional information about firewall and port requirements can be found in the [Prerequisites to Deployment](#) on page 28 section.

Cloud-enabled switches and APs communicate with ExtremeCloud for management, configuration and reporting. Cloud-enabled switches and APs place user payload traffic directly on your network. No user network traffic is communicated to the cloud; only analytics are captured and communicated to the cloud.

Deployment scenarios include, but are not limited to:

- [AP and cloud-enabled switch environment](#)
- [AP and non-cloud switch environment](#)

AP and Switch Environment

ExtremeCloud-enabled switches provide the optimal access solution for cloud-enabled ExtremeWireless APs. The cloud-switches require little configuration when used to provide the wired network access layer for the supported cloud-enabled APs. Larger deployments will benefit using both cloud-enabled switches and access points.

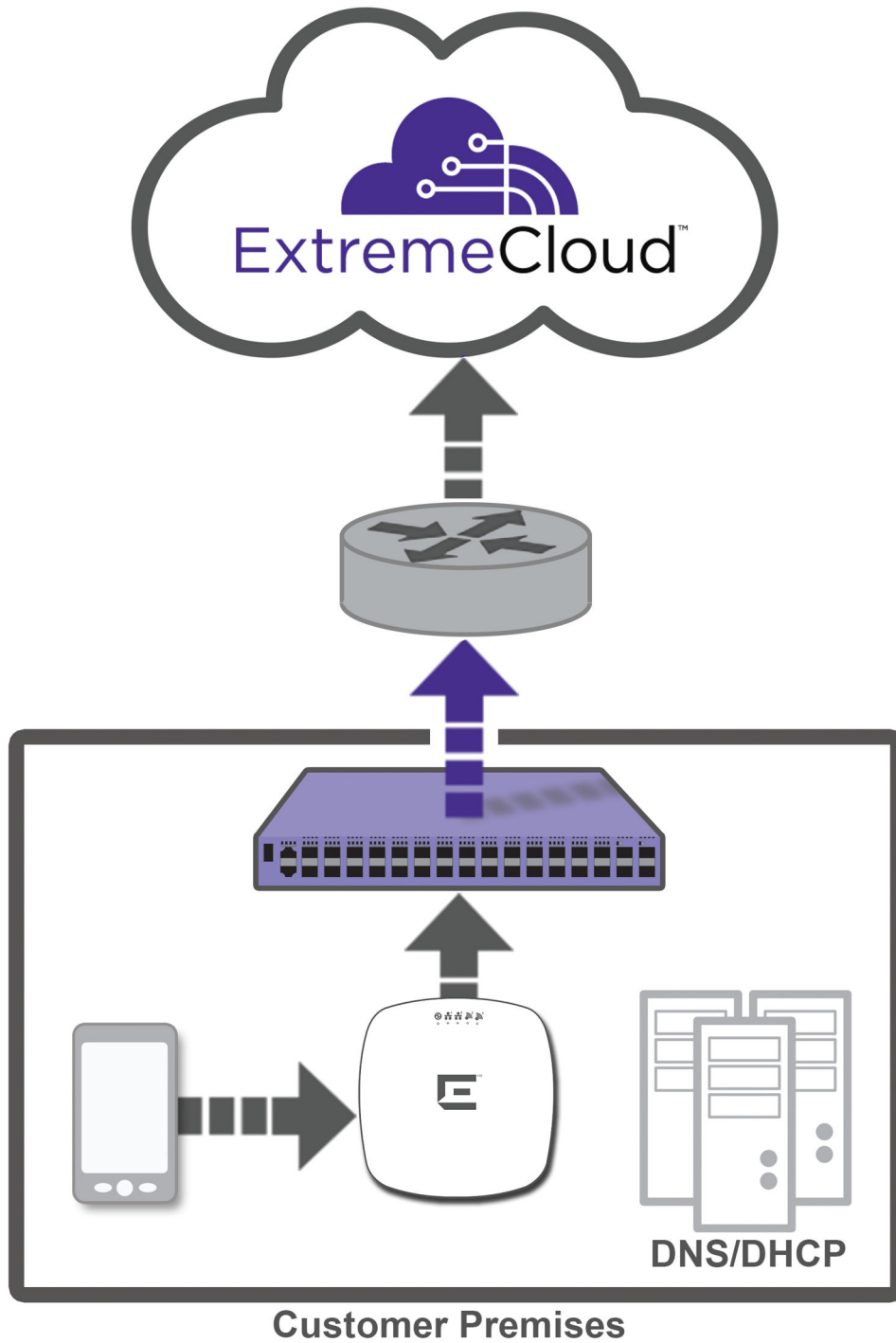


Figure 1: ExtremeWireless AP and Switch Environment

ExtremeWireless AP and Non-Cloud Enabled Switch Environment

Significant simplifications can be realized by deploying cloud-enabled ExtremeWireless APs and switches together. However, there is no requirement to use ExtremeCloud-enabled switches. This option

can be sufficient for smaller deployments. You can deploy cloud-enabled ExtremeWireless APs in your environment with existing switches that are not ExtremeCloud-enabled. The cloud-enabled APs will communicate with ExtremeCloud through the switch, but the switch will not be manageable from the ExtremeCloud user interface. Instead, you will continue to manage your switch through the existing software interface.

Topology Manager

Topology Manager is a feature in the user interface that visualizes your topology.

Topology Manager monitors the network topology state for physical devices, showing L2 switch interconnects and the end device connections to the switch. The data is displayed in the user interface using a physical layer diagram to show a switch and what is connected to each port. Zoom in and out to see the state of nodes and edge devices in a network.

More Information

- [Use Topology Manager](#) on page 54

Access Points

ExtremeCloud supports both ExtremeWireless and ExtremeWireless WiNG access points (APs). Not all models are supported. For a list of supported APs, see the *ExtremeCloud Release Notes*.

ExtremeCloud securely stores the software images that cloud-enabled devices require. When an upgrade is required, ExtremeCloud tells the AP to download the image from its secure location. All interactions between ExtremeCloud and the APs are secured with HTTPS.

APs check in to ExtremeCloud at one-minute intervals. Configuration changes and any upgrade instructions are sent to the APs in response to checking in.

Cloud-enabled APs are capable of discovering both ExtremeCloud and on-premise wireless controllers. The first manager to accept the AP will own that device for management until either it releases the device or until the AP is factory reset. If you are running a network that uses both cloud-managed and on-premise controller-managed APs, turn off automatic approval mode on the controller.



Note

For information about configuring an on-premise controller to accommodate cloud discovery, see [Prerequisites](#).

ExtremeXOS Switches

ExtremeCloud supports the management of cloud-enabled ExtremeXOS switches. For information about which switch models are supported, see the *ExtremeCloud Release Notes*.



Note

Extended Edge switching is also supported. For more information, see [Extended Edge Switches](#).

10GB licensing is available.

Switches are typically managed using the graphical user interface. Individual switches can also be managed using ExtremeCloud [CLI mode](#).

The use of cloud-enabled ExtremeXOS switches is optional. For example, if your environment already has a non-supported switch and you add ExtremeCloud-supported APs to your environment, you can use ExtremeCloud to manage the supported APs but not the switch. Or your deployment can consist of access points only.

ExtremeCloud securely stores the software images that cloud-enabled devices require. When an upgrade is required, ExtremeCloud tells the switch to download the image from a secure location on the Internet. All interactions between ExtremeCloud and the switches are secured with HTTPS.

Switches check in to ExtremeCloud at one-minute intervals. Configuration changes and any upgrade instructions are sent to the switches in response to checking in.

Policies are enforced on the APs, not on the switches.

Only switches with the ExtremeCloud built-in cloud connector and factory-installed certificates can use this product.

**Note**

For a list of cloud-enabled switches, see the [ExtremeCloud Release Notes](#).

Depending on the model, the following switch features are supported:

- PoE configuration (on p-type models)
- 802.1q VLAN support
- LACP LAG
- MLAG
- LLDP
- SNMP
- Remote syslog
- Spanning tree MSTP
- EEE
- Port throughput and error statistics
- IGMP Snooping (disabled by default)

X465 Switch Features

In addition to the features listed earlier, the cloud-supported X465 switch models include these additional features:

- PoE - 802.3af, 802.3at, 802.3br (depending on the model and PSU)
- PSUs:
 - 350W (465-48T only)
 - 715W
 - 1100W
 - 2000W

- Second power supply (additional capacity)

More Information

- [10 Gbps Licensing on Switches](#)
- [Connect Switches](#) on page 34
- [CLI Mode](#) on page 156

Extended Edge Switches

Extended Edge Switching utilizes ExtremeXOS switch models that are capable of acting as a controlling bridge to other switches. ExtremeCloud supports some of the X465, X590, and X690 models that can be used in an Extended Edge architecture.

Extended Edge Switching simplifies the deployment of and operation of edge switches, especially across a campus switched network. Based on the IEEE 80 2.1BR specification, Extended Edge Switching collapses multiple network layers into a single-tier unified services architecture that can greatly reduce the complexity of the traditional two and three-tier switch architectures.



Note

For information about which switch models are supported, see the [ExtremeCloud Release Notes](#) or the [ExtremeCloud Hardware/Software Compatibility Matrices](#).

10GB licensing is available.

Switches are typically managed using the graphical user interface. Individual switches can also be managed using ExtremeCloud [CLI mode](#).

Extended Edge Switching uses Virtual Port Extender (VPEX) architecture, comprising one or two controlling bridges (CBs), and one or more bridge port extenders (BPEs). For more information, see [VPEX Switching Architecture](#).

Zero Touch Provisioning (ZTP) performs the following tasks automatically:

- Determines if the switch is capable of being a CB.
- Detects if any BPE are attached.
- Enables VPEX mode on the CB.
- Assigns the next available slot number to each BPE.
- Configures the CB port(s) where the BPE(s) are connected to be LAGs.
- Upgrades the CB and VPEX, when upgrades are available.

More Information

- [Connect Switches](#) on page 34
- [10 Gbps Licensing for Switches](#) on page 39
- [CLI Mode](#) on page 156

VPEX Switching Architecture

Virtual Port Extender (VPEX) Description

The following figure shows the VPEX switching architecture, based on the IEEE 802.1BR specification, comprising one or two controlling bridges (CBs), and one or more bridge port extenders (BPEs) (see [Bridge Port Extender \(BPE\) Description](#) on page 17). In this document, BPEs are V400 Virtual Port Extenders, and CBs are ExtremeXOS switches.

In this architecture, ports on the CB or BPEs connecting to BPEs are termed *cascade ports*, while corresponding ports on BPEs connecting them to the CB or upstream BPEs are termed *upstream ports*. Ports from the BPEs connected to the rest of the network are termed *extended ports*.

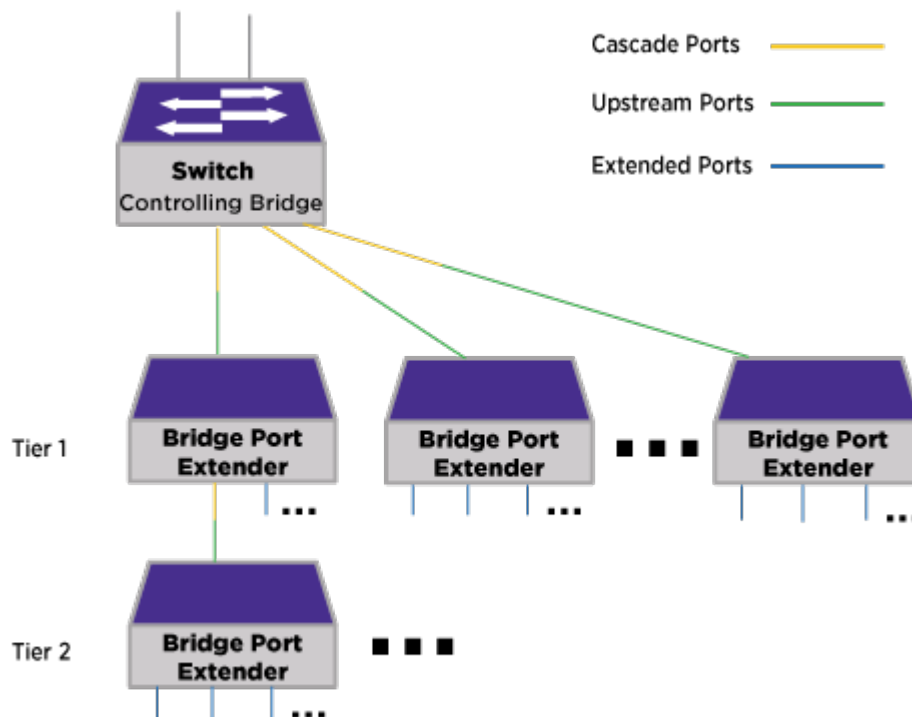


Figure 2: VPEX Architecture

Bridge Port Extender (BPE) Description

Bridge port extenders (BPEs) are devices that do not fully process packets, nor make forwarding or filtering decisions. Instead, BPEs simply receive packets from extended ports and forward packets towards the upstream controlling bridge for L2/L3 processing.

Note



Due to the lack of extensive processing performed on BPEs, traffic entering on a BPE extended port that is destined to exit another extended port on the same BPE is forwarded to the controlling bridge (CB), and then forwarded back to the BPE, rather than processed exclusively within the BPE.

Important Terminology

The following terms are important for understanding virtual port extenders (VPEX):

- **Bridge Port Extenders (BPEs)**— Devices that do not fully process packets, nor make forwarding or filtering decisions. Instead, BPEs simply receive packets from extended ports and forward packets towards the upstream controlling bridge for L2/L3 processing.
- **Cascade port**—A port on a controlling bridge or BPE that connects to an upstream port.
- **Controlling Bridge (CB)**—In this context, a switch that provides full L2/L3 packet processing and filtering functionality for cascade ports and extended ports. CBs discover their BPEs through LLDP. The CB, with its managed BPEs, acts as like a single switch, but with many more ports.
- **E-Channel-ID (E-CID)**—Identifies the BPE destination port (or port-list for multicast E-CID).
- **E-Tag**—A tag header immediately following the 802.1BR EtherType (0x893F) that contains the E-CID; this tag is only resident between bridge port extenders and controlling bridge devices.
- **Edge Control Protocol (ECP)**—Provides basic acknowledgment and re-transmission mechanism for reliable delivery; used for PE-CSP transmission.
- **Extended bridge**—A controlling bridge combined with one or more BPEs. The extended bridge is managed as a single entity.
- **Extended ports**—Ports from BPEs connected to the rest of the network. Extended ports do not operate as a Cascade Port or an Upstream port.
- **Port Extender Control and Status Protocol (PE-CSP)**—Simple command/response protocol that allows a controlling bridge to discover, program, and obtain status from a bridge port extender.
- **Upstream port**—Port on a BPE that connects to a cascade port.
- **Virtual Port Extender (VPEX)**—A switching architecture based on the *IEEE 802.1BR* specification, comprising a CB, and one or more BPEs.

For more in-depth information about VPEX switching architecture, see the *ExtremeXOS User Guide*.

Bridge Port Extender General Limitations

- In the Extended Edge Switching architecture, Layer-2, Layer-3, multicast, and filtering operations take place on the controlling bridge. The controlling bridge switch and attached BPEs constitute a single, extended switch system. Therefore, the Extended Edge Switching system assumes the scale and limits from the specific controlling bridge model in use. For applicable limits, see the Limits tables in the *ExtremeXOS Release Notes*.
- Certain ExtremeXOS features are not supported or have limitations. For information, see ExtremeXOS Feature Compatibility with V400 Virtual Port Extenders in the *ExtremeXOS 22.6 User Guide*.
- A maximum of 48 attached BPEs is supported.
- A maximum of 4 levels (tiers) of cascaded BPEs is supported.
- A maximum of 4 upstream ports (in a LAG) per BPE is supported (with V400-48).
- Stacking cannot be enabled with VPEX enabled.

Redundant Controlling Bridges

For added resiliency and redundancy, the VPEX architecture allows you to form an extended bridge using multiple controlling bridges (CBs).

You can use MLAGs to form an extended bridge with two CBs, also serving as MLAG peers, connected to dual-homed BPE devices using MLAG cascaded ports.

Note

Important considerations:



- When using MLAG, you must run LACP on the CB MLAG cascade ports.
- Jumbo frame should be enabled on the ISC ports.
- With an MLAG/VPEX topology, captive portal web-redirect does not work with ONEPolicy default resource profile. Use the profile-modifier feature to free up ACL resources from any specific policy profile (see the *ExtremeXOS User Guide* for Platform Rule Allocation).

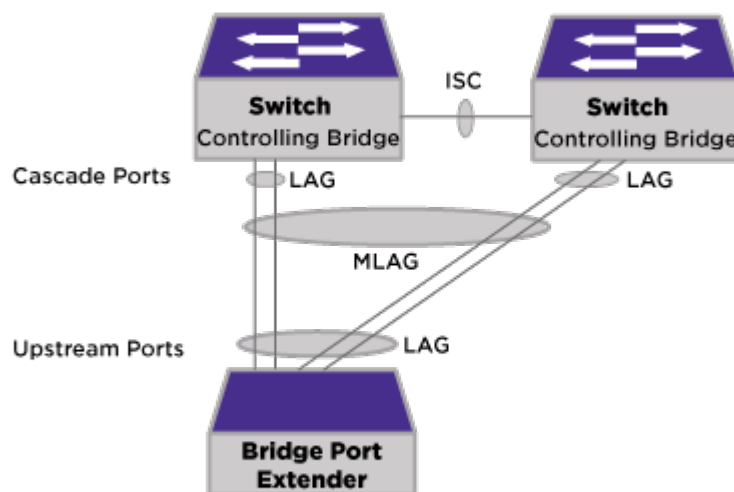


Figure 3: Redundant Controlling Bridge Architecture with MLAG over Cascaded Ports

With redundant CBs attached to each BPE, the associated extended port configuration must be identical on each controlling bridge. To reduce the configuration complexity and to minimize the risk of inconsistency, you can use orchestration mode so that any configuration commands are now checkpointed to the MLAG peer switch. Before entering orchestration mode, ensure that any configuration parameters (connecting ports for the BPEs, VLAN names, numbers etc.) are the same for both CBs.

When using automation to set up redundant CB MLAGs, the following occurs:

- The same slot number is assigned to the same BPE on both CBs.
- MLAG port is configured for first tier BPEs. The MLAG port identifier is set to 5,000 plus the BPE's slot number.

NAT Branching

Deployments of managed access points (APs) and switches behind Network Address Translation (NAT) are fully supported.

APs will connect to the cloud on port 443. If the cloud captive portal is used, the APs will also send messages to ports 1812 and 1813.

Site Management Protocol

A *site* is a collection of access points (APs) that exchange information about their client hosts to facilitate seamless roaming between APs. Sites can have associated cloud-managed switches. Typically a site will be mapped to a location. For example all the cloud-managed APs and switches on the floor of a building might be treated as one site.



Note

A site that contains ExtremeWireless WiNG APs will not contain ExtremeWireless APs. Also, a site will not combine ExtremeWireless WiNG 5 and 7 model access points. The configuration options that display depend on the type of APs deployed at the site.

Site definition and corresponding services are managed through the ExtremeCloud user interface. A default site is created for you when your first purchase an entitlement. When your APs discover ExtremeCloud, they are added to this default site. Services are assigned when an AP discovers the cloud service. You can reassign the APs to another compatible site, but an AP can be assigned to one site only. There is a maximum limit of 100 APs per site.

ExtremeWireless APs in a site exchange user information using SIAPP, a specialized multicast-based protocol. ExtremeWireless WiNG APs in a site exchange information using MiNT. MiNT and SIAPP are specialized administration protocols. You must allow MiNT or SIAPP traffic on the segment hosting your APs.

SIAPP is a multicast protocol that sends packets to **224.0.1.178, Port: 3517**. (Switches do not participate in SIAPP, although they may forward SIAPP frames as they would other multicast protocols.) Session information is shared for all users states (such as authentication state, assigned policies) and band steering.

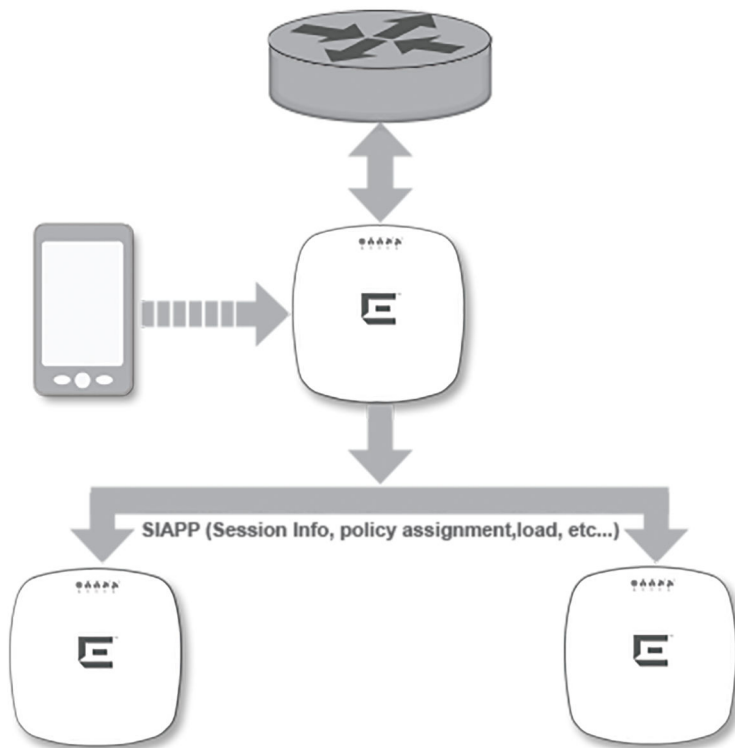


Figure 4: SIAPP Site Exchange

Layer 2 MiNT packets use the ether-type **0x8783**. Layer 3 MiNT packets use UDP port **24576**.

Without L2 connectivity between ExtremeWireless APs in a site, roaming and site ACS will not work properly. The APs within a site operate within a single RF domain and therefore must have L2 connectivity to function properly.

It is a best practice to use a single VLAN for all of the APs in a site. However, if you prefer to distribute the APs within a site over multiple VLANs, then you must allow either routing or forwarding of SIAPP multicast between those VLANs.

No additional grouping is needed for load balancing.

If you need to deploy APs on different subnets and want to allow roaming between the APs, then you must configure your routers and switches to allow SIAPP or MiNT messages between the subnets.

Multiple Site Support

Seamless inter-AP roaming is supported only between the APs in a site. For this reason, you should create your site so that the devices correspond to a physical location. For example, you can create a site consisting of all the devices on a floor or in a building.



Note

For information about the number of sites supported, see [System Limits](#) on page 31.

Different sites can have the same configuration or have distinct configurations. However, transparent roaming is only available between APs in a site, and not across multiple sites.

The authentication infrastructure (RADIUS server) can be either local to the site or reachable by the network.

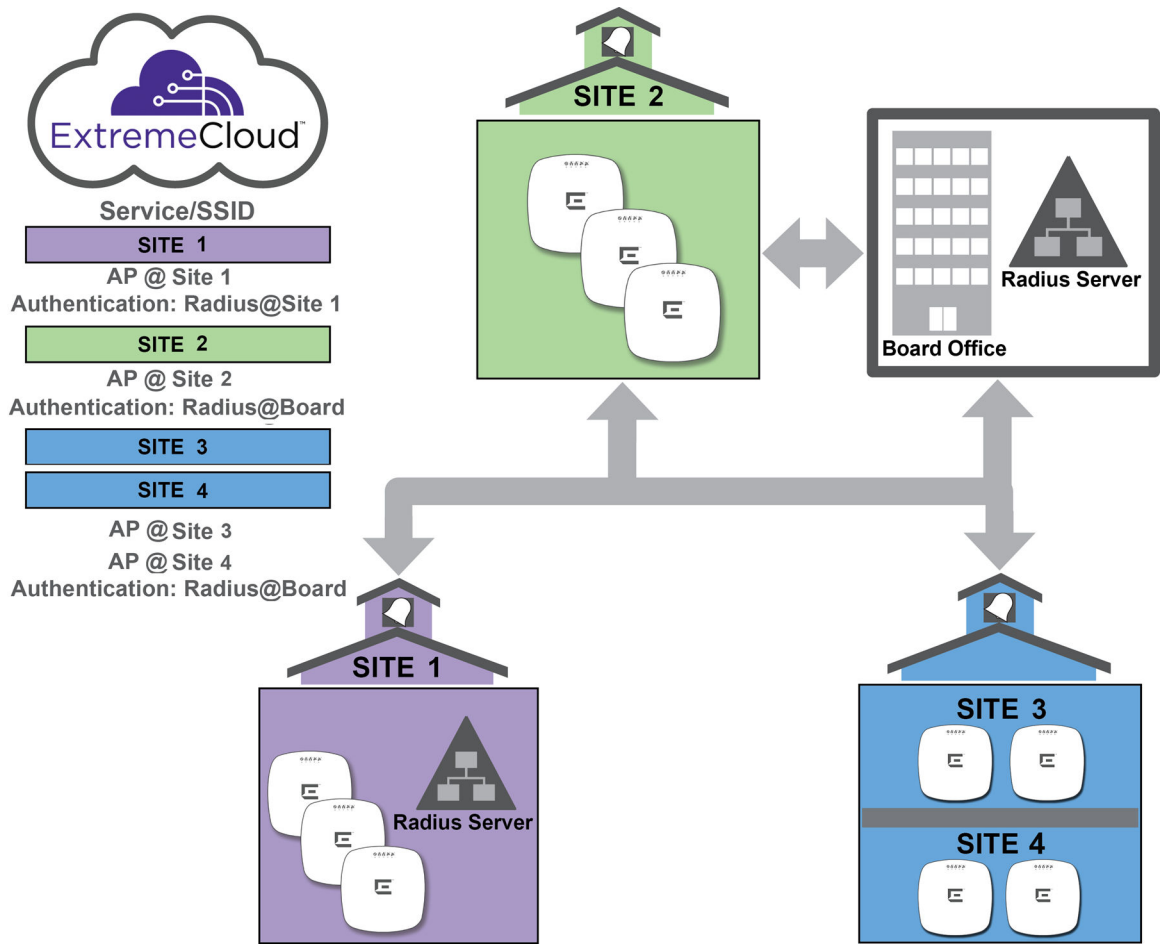


Figure 5: Multiple site deployment for a school board managing several independent schools

Authentication

The AP is responsible for all client (user) engagement, including authentication. ExtremeCloud supports the following authentication mechanisms with both ExtremeWireless and ExtremeWireless WiNG APs:

- WPAv2 PSK
- WPAv2-Enterprise with RADIUS
- MAC-Based Authentication
- Captive Portal



Note

Although WEP and TKIP encryption are also available, we do not recommend or endorse using them due to the security flaws that are inherent with WEP.

WPAv2 PSK and WPAv2-Enterprise Authentication

WPAv2 PSK and *WPAv2-Enterprise with RADIUS* authentication provides privacy based on the IEEE standard. The privacy settings are editable for both methods.

WPAv2 PSK

Access is allowed to any client that knows the pre-shared key. All data exchanged between the client and the AP will be AES encrypted from keys using the common, shared secret.

If MAC-based authentication (MBA) is also enabled, you can assign different roles to different devices with PSK because MBA can distinguish between different devices. If MBA is not enabled, then devices with PSK use the Default Unauth role only.

WPAv2-Enterprise with RADIUS

This method supports 802.1x authentication with a RADIUS server, using AES encryption. This is the highest degree of security for networking, particularly when used in conjunction with client certificate-based authentication (EAP-TLS). All 802.1x protocols are supported.

Although a RADIUS server is not required to use ExtremeCloud, you can configure site localized (reachable) RADIUS settings for 802.1x services. Users in the branch will authenticate with local authentication servers. Access control, roles and policy are enforced by the AP based on the RADIUS responses.

RADIUS servers can be configured to provide authentication or [MAC-based authentication](#).

MAC-Based Authentication

MAC-based authentication enables network access to be restricted to specific devices identified by a MAC address.

A RADIUS server is required for MAC-based authentication. Each device that is to be authenticated by MAC-based authentication must have an entry in the RADIUS server database. The user ID of the entry is the device's MAC address. The password of the entry is either a fixed password shared by all devices using the network or the device's MAC address. You must configure ExtremeCloud so that it knows whether to use the device's MAC address as its password or a password that is used with all devices undergoing MAC authentication.

To set up a RADIUS server for MAC-based authentication, you must set up a user account with user ID=MAC and Password=MAC (or a password defined by the administrator) for each user. Specifying a MAC address format and role depends on which RADIUS server is being used.

MAC-based authentication can be used on its own, or in conjunction with either WPA-PSK or external captive portal. When MAC-based authentication is used with external captive portal, the RADIUS server typically needs to have a second user ID and password configured for use by the client while authenticating to the captive portal.

The RADIUS server can respond to a request for MAC-based authentication by returning the name of a policy that it wants applied to the supplicant client's traffic. The name must be the name of a policy defined in ExtremeCloud and deployed to the AP that is performing authentication.

By itself, MAC-based authentication does not provide privacy (encryption between AP and client device). However, it can be used with WPAv2-PSK and WPAv2 Enterprise, which do provide privacy.

Captive Portal

ExtremeCloud offers two captive portal options:

- Built-in captive portal feature
- External captive portal (ECP) that redirects to a third-party server for authentication

You can [create a walled garden](#) using either captive portal option.

When captive portal is enabled, cloud-enabled APs intercept the HTTP and HTTPS traffic of unauthenticated users and redirects them to the captive portal splash screen. The captive portal can then authenticate the user. (Authentication can be as simple as asking the user to select a button to accept any terms and conditions for using the network or it can ask the user for credentials.) If the user passes the captive portal criteria, the captive portal tells the cloud-enabled AP to allow the user onto the network. The captive portal can also assign the user to one of the access control policies that is configured on the AP.

ExtremeCloud supports captive portal that is firewall friendly. All interactions with the captive portal take place through port 443 or port 80, which are routinely allowed to egress firewalls. This product also supports captive portals that are on the same side of the firewall as the AP.

For an external captive portal, the DHCP IPv4 address pool used by unauthenticated clients must be large enough to provide additional IP addresses to all APs configured with ECP. This is because each AP creates a virtual interface on each non-authenticated policy VLAN and assigns an IP address to it from the pool.

More Information

- [How to Configure a Captive Portal](#) on page 182
- [Configure General System Settings](#) on page 224

Layer 7 Application Control

This product supports Layer 7 application control, performed by the flow-based Deep-Packet Inspection (DPI) engine on the access points. The DPI engine core is the same engine used with ExtremeControl and ExtremeAnalytics, and uses the same Application ID database, containing over 3300 fingerprints and identifying over 2,000 distinct applications.



Note

The DPI engine recognizes hundreds of distinct applications.

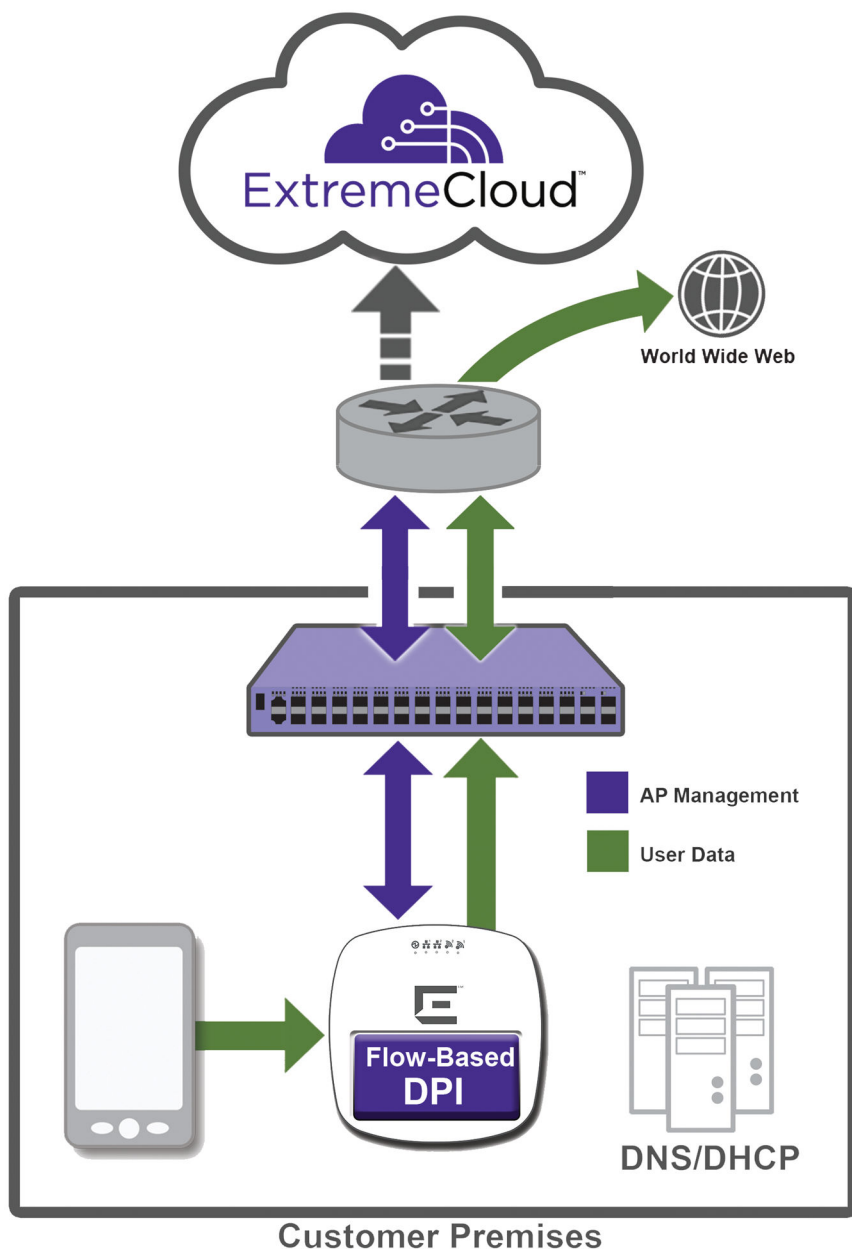


Figure 6: Flow-based Application Control

Policy enforcement is extended to IPv6 traffic, with similar capabilities for advanced rule syntax as IPv4 rules. However, the Redirect action is only available for IPv4.

Applications policies and rules are configured using the ExtremeCloud management interface. Applications are organized as groups, and the actions that are applied to a group are applied to all of the applications in that group.

If you are administering a multi-tenant environment, the application policies that you create for one tenant are not shared with other tenants.

More Information:

- [Application Policies and Rules](#)
- [Configuring Application Rules](#)
- [Configuring Extended Application Rules](#)

Statistics and Reporting

Statistics data is aggregated into 15-minute reporting intervals. APs also report device fingerprinting (device vendor and OS information). No user data is communicated to the cloud.

Any configuration changes affecting statistics will not be visible in the dashboard until the next reporting cycle.

**Note**

See the [ExtremeCloud Release Notes](#) for information about requirements and limitations.

Extreme AirDefense Integration

A cloud-managed access point (AP) can integrate with the Extreme AirDefense® Service Platform, which allows the AP to function as an AirDefense sensor, or to act as a sensor and retain the ability to forward traffic.

In dedicated sensor mode, the AP operates independently from **ExtremeCloud** while **ExtremeCloud** continues to see the AP and display the AP role as a dedicated AirDefense sensor. In its role as a dedicated sensor, the AP does not report statistics to the **ExtremeCloud**.

Licensing issues and reporting are handled on the AirDefense servers. Traffic is configured on the APs through **ExtremeCloud**.

Configure an AirDefense profile by selecting **Configure > Sites > Air Defense**. The profile is assigned to all APs at the site.

If a site is deleted, the associated profile is deleted.

More Information

[Configure AirDefense Profiles](#) on page 104

ExtremeLocation Integration

ExtremeCloud provides location analytics by integrating with ExtremeLocation. Additional licensing is needed to access ExtremeLocation. Licensing enforcement is managed by ExtremeLocation.

ExtremeLocation is a cloud-based 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 the AP WebSocket.

After you enable location analytics in ExtremeCloud, users can log in to ExtremeLocation directly from the ExtremeCloud user interface.

All access points (APs) at a ExtremeCloud site can be configured to use ExtremeLocation. ExtremeCloud allows one device group per site.

APs receive the configuration to report to ExtremeLocation when they check in to ExtremeCloud. The report data itself is sent from the APs directly to ExtremeLocation. The report data is not seen by and does not pass through ExtremeCloud

Individual APs can have radios put into sensor mode. For some AP models, if the radio is not in sensor mode but it is serving ExtremeLocation, the AP can also be configured for either Promiscuous or Hop Off Channel modes. For information about which models support these advanced options, see the Release Notes.

ExtremeCloud and ExtremeLocation are configured separately and maintain separate floor plan configurations.

More Information

- [How to Enable Location Analytics](#) on page 106

3 Connecting Your Devices to ExtremeCloud

Prerequisites to Deployment
System Limits
ExtremeCloud License Expiration
Create or Update Your Account
Use the Deployment Prerequisite Tool
Device Adoption Rules
Connect Switches
Connect Access Points

This chapter describes the prerequisites you must meet and how to connect your devices to **ExtremeCloud**.

Prerequisites to Deployment

The following prerequisites must be met before you can register your devices:

- Purchase and receive a supported device.
- Locate the Welcome email with a service contract number.



Note

Former Azara users do not receive or require a contract number.

- Forward the Welcome email to your network administrator.
- Identify the location and site where the device will be deployed.
- Meet the [network requirements](#).
- Meet the additional requirements stated in the [ExtremeCloud Release Notes](#).



Note

If your existing network is also using Extreme Networks wireless controllers, you must configure the controllers to accept only the manually approved access points (APs). This action prevents the cloud-enabled APs from connecting to the controller. Note that the AP connection is not predicted in the case of both an on-premise controller and the cloud server accepting an AP.

Network Requirements

You must meet the following network requirements:

- Make sure your company has configured one or more Dynamic Host Configuration Protocol (DHCP) servers that can issue IP addresses and a Domain Name System (DNS) server address to ExtremeCloud-managed APs, switches, and both wired and wireless users.
- HTTPS traffic must be allowed through your firewall on port 443 towards devices.extremenetworks.com. This allows ExtremeCloud-managed APs and switches to connect to ExtremeCloud to receive configuration and software updates, and to send analytics.
- Make sure that your content filter is allowing access to Amazon Web Services (AWS).
- Verify that Network Time Protocol (NTP) is allowed out through your firewall on port 123 so that the APs can submit NTP queries to pool.ntp.org to set their clocks.
- Each site must have L2 connectivity. The APs within a site operate within a single RF domain and therefore must have L2 connectivity to function properly.
- The best practice is to use a single VLAN for all the APs in a site instead of distributing the site's APs over multiple VLANs. If you decide to distribute a site's APs over multiple VLANs, then you must allow either routing or forwarding of SIAPP multicast between those VLANs.

ExtremeCloud-enabled devices need to be able to access several different application servers in order to provide their full functionality. Verify that your firewall is allowing ExtremeCloud-enabled devices behind it to access to the following domains and ports:

Table 4: Firewall Requirements and Port List

Component		Ports for AP/Cloud Communication					
Source	Destination / Domain Name	Protocol	Src Port	Dest Port	Service	Remark	Open Firewall
Admin Console	ezcloudx.com	TCP	Any	443	HTTPS	Access the ExtremeCloud management application.	Required
Admin Console / API integrated systems	api.ezcloudx.com	TCP	Any	443	HTTPS	Application access to the backend services managing ExtremeCloud-enabled devices.	Required
Access Point & Switches	devices.extremenetworks.com	TCP	Any	443	HTTPS	Management Tunnel between AP and ExtremeCloud (configuration, image, statistics, upgrade, traces).	Required
Access Points & Switches	NTP Server	UDP	Any	123	NTP	Clock synchronization.	Required
Access Points	radius.ezcloudx.com	UDP	Any	1812, 1813	RADIUS	The integrated captive portal solution requires a cloud RADIUS lookup for each wireless client authentication using the captive portal.	Required if using the built-in captive portal

Table 4: Firewall Requirements and Port List (continued)

Component		Ports for AP/Cloud Communication					
Source	Destination / Domain Name	Protocol	Src Port	Dest Port	Service	Remark	Open Firewall
Access Points	cp.ezcloudx.com	TCP	Any	443, 80	HTTP, HTTPS	Used by the integrated captive portal solution hosted at cp.ezcloudx.com. Access to the portal is required to ensure wireless clients can authenticate using the captive portal.	Required if using the built-in captive portal
Access Points & Switches	http://aptransient-eu-central-1.s3.eu-central-1.amazonaws.com/	TCP	Any	443	HTTPS	Used by ExtremeCloud-enabled devices that, on command, may upload tech support files to storage managed by this application.	Required
Access Points & Switches	http://extremeimages.s3.amazonaws.com/	TCP	Any	443	HTTPS	Required to successfully upgrade ExtremeCloud managed devices. The IP range for the S3 bucket is: <pre>{ "ip_prefix": "52.219.72.0/22", "region": "eu-central-1", "service": "S3" }, { "ip_prefix": "52.219.44.0/22", "region": "eu-central-1", "service": "S3" } { "ip_prefix": "52.92.68.0/22", "region": "eu-central-1", "service": "S3" }, { "ip_prefix": "54.231.192.0/20", "region": "eu-central-1", "service": "S3" },</pre>	Required

Table 4: Firewall Requirements and Port List (continued)

Component		Ports for AP/Cloud Communication					
Source	Destination / Domain Name	Protocol	Src Port	Dest Port	Service	Remark	Open Firewall
Any	Access Point	TCP	Any	2002, 2003	RCAPD	Collect WireShark traces using AP Real Capture, if enabled.	Optional
WiNG APs	mgmt.devices.extremenetworks.com	TCP	Any	443	HTTPS	Management tunnel between WiNG AP and ExtremeCloud	Required - Allows outbound connections from devices to ExtremeCloud over the various ports listed. This is typically not an issue as these ports are usually open already.

System Limits

The following table shows the system limits:

Table 5: System Limits for ExtremeCloud

Item	Maximum Number
Accounts per customer	1
Sites per account	2,500
Access points per account	10,000
Switches per account	Unlimited
Access points per site	100 ExtremeWireless / 128 ExtremeWireless WiNG
Switches per site	Unlimited
User per site	2,000
Roles per access point	64
Rules per role	64
Active networks per account	8
Administrator accounts per customer	20
Rate limiters per account	16 (8 inbound and 8 outbound)
Rate limiters per site	16 (8 inbound and 8 outbound)
MAC addresses in a customer blacklist	768

ExtremeCloud License Expiration

ExtremeCloud expiring licenses are handled as follows:

- 90-day warning in the user interface **before** the license expires:
 - Warnings display in the heading of the main dashboard
 - View the list of expiring entitlements under **Administration > System > Expiring Entitlements**
- During the 90 days **prior** to license expiry, **ExtremeCloud** provides the device with full functionality. After the license expires, the device is not eligible for support and its configuration cannot be changed.
- 90-day grace period to renew the license **after** the license expires. The devices are not configurable during the grace period.
- After the 90-day grace period expires:
 - The device is completely ignored. It cannot be configured, and its statistics and events are discarded.
 - All cloud-managed devices will start trying to discover an Extreme Networks cloud manager as if it never had a manager before.

If you choose to renew the license after it expires, the device can recover the cloud configuration if your account has not been eliminated and if **ExtremeCloud** has not deleted your data. If you have other devices at the same site that you are adding the renewed device to, the renewed device will receive the current configuration of the other devices. This configuration may be different than the renewed device had before its license expired.



Note

For information about licensing in product integrations, such as ExtremeLocation, see the product-specific documentation.

Create or Update Your Account

Whether you are creating a new ExtremeCloud administrator account or are adding a device to an existing account, follow these steps:

- 1 Locate your Welcome email from ExtremeCloud.
- 2 Select the activation link in the Welcome email and follow the on-screen instructions.



Note

(Optional) You can [add two-step verification for added security](#).

Proceed to [using the Deployment Prerequisite tool](#) and connecting your devices.

Use the Deployment Prerequisite Tool

An administrator can download and run a prerequisite tool to verify that installation requirements have been met before installing cloud-managed access points and switches at a site. The tool checks requirements specific to **ExtremeCloud** and performs tasks such as making REST API calls to your REST servers, looking up your FQDNs in DNS, and verifying that your Amazon S3 connection is enabled.

This tool is compatible with Windows, Linux, and Mac OS X devices.

To download and use the prerequisite tool:

- 1 Locate your contract number and Welcome letter. Keep these on hand as you will need to enter this information to use the tool.
- 2 Log on to the machine that is on the same subnet that your access points (APs) are deployed on. You will need to run the executable file on this same subnet.
- 3 Download the zip file (ezcloud_prerequisite_validation_tool.zip), which contains the tool in the form of binary executable files, a Readme, and a license file. The link to download the zip file is available from the following locations:
 - On the **ExtremeCloud** login screen in the bottom right corner.

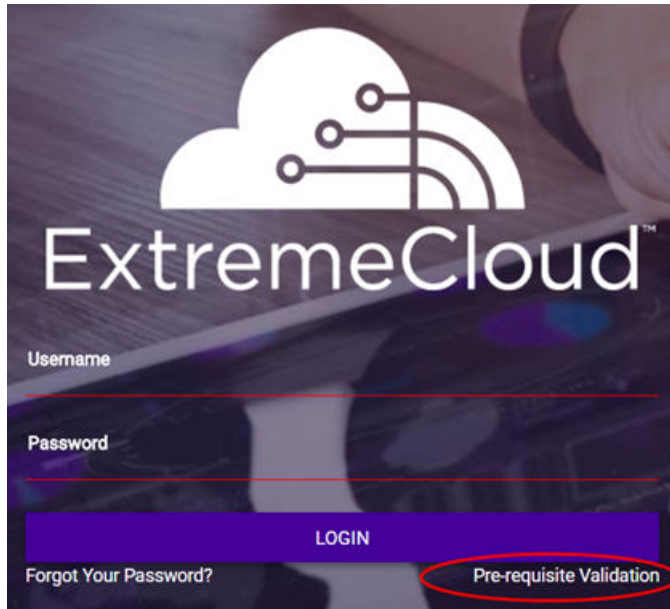


Figure 7: Login Screen

- From the drop-down list located on the top right corner of the user interface, under your user name.

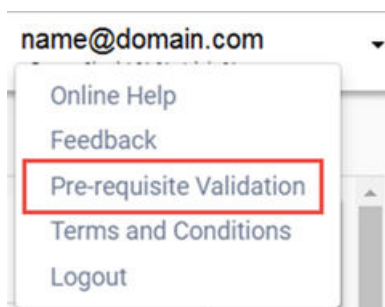


Figure 8: Drop-down List

- 4 Run the binary executable file that is suitable for your operating system (Windows, Linux, Mac OS X).

The tool checks the local machine and a summary report is returned. All of the items on the list must pass the test in order to deploy the product. If any item fails, fix it and then repeat this procedure until everything passes. Then proceed with deployment of your devices.

```

2018-07-31T17:23:15.957Z: SUCCESS

Prerequisite Tool Verification Summary

TESTS                                     RESULT
-----                                     -
TEST1: DHCP AND DNS SERVER CONFIGURATION  PASSED
TEST2: EZCLOUD SPECIFIC FQDN DNS RESOULTION PASSED
TEST3: NTP SYNC                           PASSED
TEST4: EZCLOUD LOGIN PAGE DOWNLOAD        PASSED
TEST5: EZCLOUD UI SERVER CONNECTIVITY     PASSED
TEST6: EZCLOUD IDENTIFY AP SERVER CONNECTIVITY PASSED
TEST7: EZCLOUD WING AP SERVER CONNECTIVITY PASSED
TEST8: EZCLOUD CAPTIVEPORTAL SERVER CONNECTIVITY PASSED

```

Figure 9: Prerequisite Tool Summary Report

Device Adoption Rules

The device adoption feature simplifies the deployment of access points (APs) and switches by automatically assigning them to a site. A set of rules determines the site assignments when devices are registered for the first time. Without adoption rules, devices must be manually assigned to sites.

To use the adoption rules feature:

- 1 Create a site (**Configure > Site**).
- 2 Configure the adoption rules for the site (**Configure > Adoption**).
- 3 Connect the devices to **ExtremeCloud**.

Connect Switches

If you will use device adoption rules, create a site with adoption rules before connecting devices.

If you are using cloud-supported ExtremeXOS switches or Extended Edge Switching in your environment, connect all of your switches before you connect the APs. ExtremeCloud-supported switches are not required to use ExtremeCloud-supported APs.

After you create an ExtremeCloud account:

- 1 Install the switch hardware and connect the power according to the product-specific *Installation Guide*.
- 2 Connect one of the switch's Ethernet ports on the front panel to a network that provides Internet access. The switch should be connected through one of its data plane ports if at all possible, rather than through its management port.



Important

For a supported switch to locate and connect to ExtremeCloud, only *one* port can be connected. Once the connection is established, additional ports can be connected.

The switch uses Zero Touch Provisioning (ZTP) to automatically connect with ExtremeCloud. If needed, the switch will download more recent firmware over HTTPS. The switch automatically upgrades its firmware, reconnects to ExtremeCloud and receives its configuration. All ports, except the management port, are placed on the same untagged management VLAN.

- 3 Verify that the management LED indicates that the switch is powered on and has completed its start-up sequence. The LED should be blinking green slowly at the rate of about once per second.
- 4 Log in to your ExtremeCloud administrator account at <https://ezcloudx.com>.
- 5 When you log in for the first time, the configuration wizard walks you through the initial configuration. Use the wizard to update the network security key of the predefined wireless network. Alternatively, you can exit the wizard and configure your own networks.
- 6 From the user interface, select **Monitor > Devices > Switches**. Look at the switch's status. Typically the switch takes a few minutes to connect with ExtremeCloud.

The status icon changes from gray (Undiscovered) to either green, yellow or red. As the switch cycles through upgrade and configuration, its state will change color in the user interface several times. The switch is ready to use when the status is either green (in service) or yellow (in service, trouble).

- 7 (Optional) If you purchased 10 Gbps licenses to enable 2 or 4 uplink ports for 10Gbps operation, you must assign them to a switch before they can be used. Select **Administration > System**. In the **Unassigned Switch Voucher** list and assign the 10GB license to the switch. Once a software license voucher has been assigned, cloud management takes care of generating the license key and applying it to the particular devices.



Note

The 10GB licenses are a separately licensed feature from the ExtremeCloud entitlement, and can be ordered at the same time you order an ExtremeCloud switch and entitlement or later.

- 8 Repeat these steps for all ExtremeCloud-enabled switches before deploying your APs.



Note

If a switch persistently fails or its status remains gray or red for more than 20 minutes, contact Support.

Connect Access Points

If you are using ExtremeWireless WiNG AP7612, AP7632, or AP7662, make sure that your firmware is upgraded to 5.9.2.2 or higher (and 5.9.2.5 is recommended) to connect to **ExtremeCloud**. For instructions, see this GTAC article: <https://gtacknowledge.extremenetworks.com/articles/Solution/ExtremeCloud-WiNG-Access-Points-not-connecting-to-ezcloudx-com> or refer to the ExtremeWireless WiNG AP-specific user documentation.

If you will use device adoption rules, create a site with adoption rules before connecting devices.

Follow this process to deploy access points (APs):

- 1 Connect your AP's LAN 1 or LAN 2 Ethernet port to either a switch that allows the AP to connect to the Internet, or connect to an Ethernet network port with Internet connection. Apply power to the AP using either PoE from the switch or a separate external transformer. For more information, see the product-specific *Installation Guide*.

The AP discovers ExtremeCloud and gets configured automatically, typically in a few minutes. When connected, the AP starts advertising the SSIDs assigned to it, initially only **Staff**. If your cellphone or laptop lists this SSID as available, then the AP has connected successfully.

- 2 Look at the physical AP and verify that the Radio 1 and Radio 2 LEDs are solid green, which indicates that the AP is activated in the cloud.

The following table shows the LED patterns and the associated status for ExtremeWireless APs when they are connected to cloud management.



Note

The AP7532 uses an adoption mode indicator instead of a green LED pattern to show adoption to ExtremeCloud.

Table 6: LED Patterns for ExtremeWireless APs Connecting with ExtremeCloud

Radio B/G LED (Left)	Radio A LED (Right)	Status LED	AP Detailed State
Off	Off	Blink green	Initialization: Power-on self test (POST)
	Blink green	Blink green	Initialization: Random delay
		Blink red	Initialization: No Ethernet
	Solid green	Blink green	Initialization: Vulnerable period (not supported)
		Blink red	Reset to factory defaults

Table 6: LED Patterns for ExtremeWireless APs Connecting with ExtremeCloud (continued)

Radio B/G LED (Left)	Radio A LED (Right)	Status LED	AP Detailed State
Blink green	Off	Blink green or orange	Network discovery: 802.1x authentication
		Blink red	Failed 802.1x authentication
	Blink green	Blink green or orange	Network discovery: DHCP
		Blink red	Default IP address
	Solid green	Blink green or orange	Network discovery: discovery/connect
		Blink red	Discovery failed
<ul style="list-style-type: none"> Green - Radio On Off - Radio Off 	<ul style="list-style-type: none"> Green - Radio On Off - Radio Off 	Solid green	Connected

The following table shows the LED patterns and the associated status for ExtremeWireless WiNG APs when they are connected to cloud management.

Table 7: LED Patterns for ExtremeWireless WiNG APs Connecting with ExtremeCloud

Task	5 GHz Activity LED (Amber)	2.4 GHz Activity LED (Green)
Unconfigured Radio	On	On
Normal Operation	<ul style="list-style-type: none"> If this radio band is enabled: Blinks at 5-second intervals If this radio band is disabled: Off If there is activity on this band: Blinks at 1 time per second 	<ul style="list-style-type: none"> If this radio band is enabled: Blinks at 5-second intervals If this radio band is disabled: Off If there is activity on this band: Blinks at 1 time per second
Firmware Update	On	Off
Locate AP Mode	LEDs blink in an alternating green, red and amber pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions.	LEDs blink in an alternating green, red and amber pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions.

- Log in to your ExtremeCloud administrator account at <https://ezcloudx.com>.
- When you log in for the first time, the configuration wizard walks you through the initial configuration. Use the wizard to update the network security key of the predefined wireless network. Alternatively, you can exit the wizard and configure your own networks.

- 5 Select **Monitor > Devices > Access Points** and look for the device in your **Devices** list. If the AP is not listed in your account, contact Support. (If a WiNG AP fails to connect, try [performing the steps in the troubleshooting topic](#) first.)

**Note**

If an AP persistently fails or its status remains gray or red for more than 20 minutes, contact Support.

4 Licensing and RMAs

10 Gbps Licensing for Switches ExtremeCloud License Expiration RMA Replacement Process

This chapter contains information about how licensing works, including grace periods and expiry. It also explains the RMA process.

10 Gbps Licensing for Switches

10 Gbps licenses are available to enable 2 or 4 uplink ports for 10Gbps operation. This is a separately licensed feature from the ExtremeCloud entitlement, and can be ordered at the same time you order a ExtremeCloud switch and entitlement or later.

After purchasing software license vouchers, you must assign them to a switch before they can be used. A message displays in the dashboard with a notification about unassigned vouchers.

Once a software license voucher has been assigned, cloud management takes care of generating the license key and applying it to the particular devices.

To assign licenses, select the dashboard message that notifies you about unassigned vouchers, or select **Administration > System** from the menu. The **Assign License** pane only displays when there are unassigned license vouchers.

ExtremeCloud License Expiration

ExtremeCloud expiring licenses are handled as follows:

- 90-day warning in the user interface **before** the license expires:
 - Warnings display in the heading of the main dashboard
 - View the list of expiring entitlements under **Administration > System > Expiring Entitlements**
- During the 90 days **prior** to license expiry, **ExtremeCloud** provides the device with full functionality. After the license expires, the device is not eligible for support and its configuration cannot be changed.
- 90-day grace period to renew the license **after** the license expires. The devices are not configurable during the grace period.
- After the 90-day grace period expires:
 - The device is completely ignored. It cannot be configured, and its statistics and events are discarded.
 - All cloud-managed devices will start trying to discover an Extreme Networks cloud manager as if it never had a manager before.

If you choose to renew the license after it expires, the device can recover the cloud configuration if your account has not been eliminated and if **ExtremeCloud** has not deleted your data. If you have other

devices at the same site that you are adding the renewed device to, the renewed device will receive the current configuration of the other devices. This configuration may be different than the renewed device had before its license expired.

**Note**

For information about licensing in product integrations, such as ExtremeLocation, see the product-specific documentation.

RMA Replacement Process

The RMA process requires that you contact Support with the serial number of the device to be replaced. Support determines whether the device is eligible for replacement, and issues an RMA number if it is eligible. When the replacement device is shipped, its entitlements are pushed to cloud management. If the device is a switch with a 10GB license, a new 10GB license is issued for the replacement switch.

The exact configuration of the original device can be cloned to the replacement device. To do so, both devices must be identical models, have identical licenses, and must exist in the orchestration product.

When you receive the new device, set it up with a cloned configuration as follows:

- 1 Install the device (access point or switch) according to the device's installation documentation.
- 2 Log in to the orchestration user interface as an administrator with Read/Write access.
- 3 (10GB licenses only) If you are replacing a switch with a 10GB license, select **Administration > General > (Miscellaneous) Activate a Contract Number** to assign the new 10GB license to the switch.
- 4 Select **Configure > Devices > <deviceType>**, and select the device that will be replaced from the list of devices.
The individual device dashboard displays.
- 5 Select **Configure <deviceType> > Advanced**. If you are replacing a switch that is in CLI mode, the new switch will be activated in **CLI mode**.

The **Advanced Settings** dialog opens.

- 6 Select **RMA**.

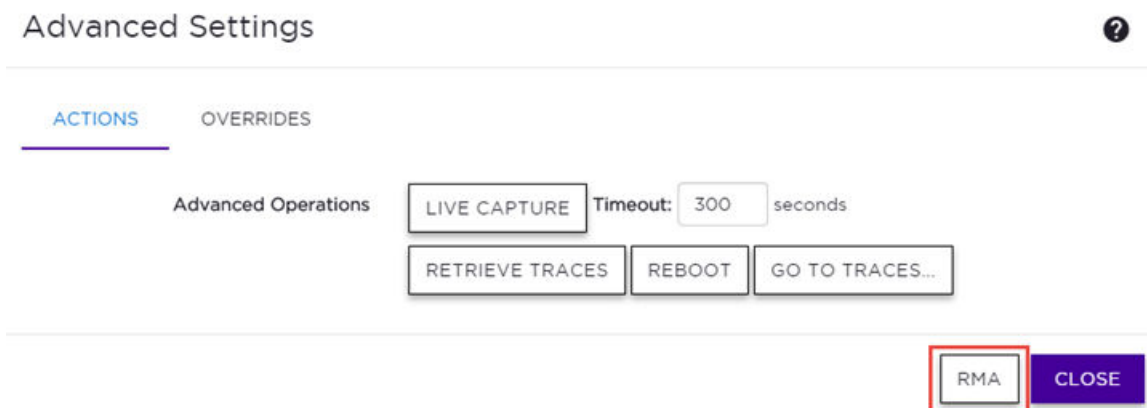


Figure 10: Advanced Settings for an Access Point

The RMA Advanced Settings dialog opens.

- 7 From the **Replacement** drop-down list, select the device you want to use as the replacement.



Note

You will receive a warning message if any licenses will be removed from the clone source, and if the source has to be removed from a site to make room for the replacement. If you do not wish to proceed, select **Cancel** to cancel the action.

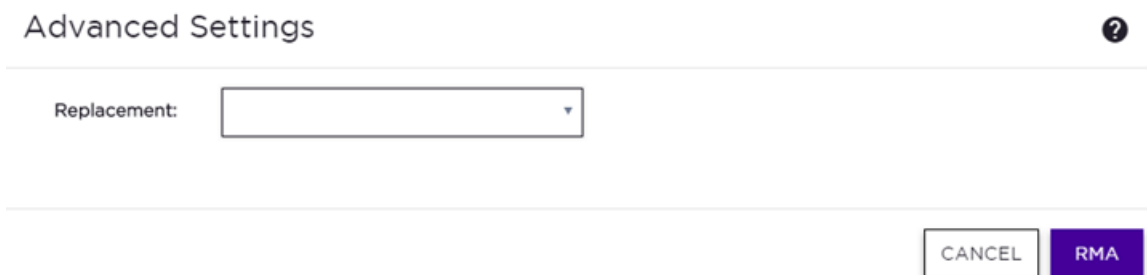


Figure 11: Example: RMA Advanced Settings Dialog

- 8 Select **RMA**.

The configuration is cloned from the original device and sent to the replacement device. The replacement device receives the configuration the next time it checks in with **ExtremeCloud**.

When the original device is returned with the RMA, the device's orchestrator entitlements are deleted and removed from **ExtremeCloud**.

5 User Interface

User Interface Details User Interface Changes

This chapter explains that layout and functionality of the user interface. It also explains the changes made to the user interface from version 4.31.01.

User Interface Details

The **ExtremeCloud** user interface has a main menu on the left side of the screen for performing network management tasks. The **Dashboard** menu item is the default view.

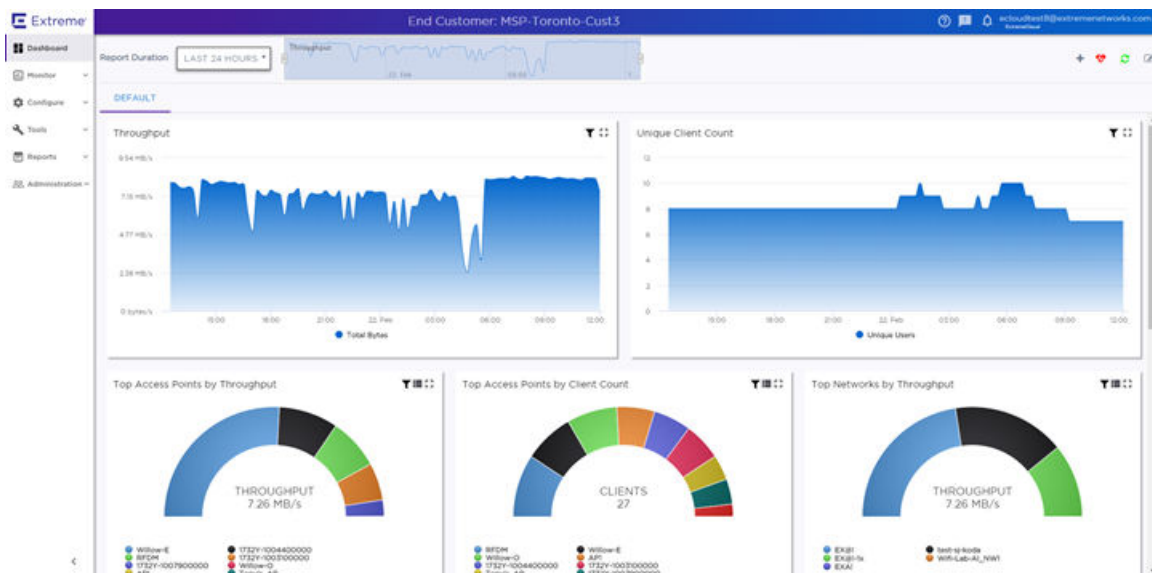


Figure 12: User Interface with the Overview Dashboard

The main menu items are:

- **Dashboard** - Shows an overview of your network activity and performance. For more information, see [Dashboard](#) on page 45.
- **Monitoring** - Provides navigation to the entity dashboards and networking associations for the following items:
 - **Sites** - View an individual site dashboard, and associated floor plans, topology, networks, devices, clients, logs, and unsanctioned APs.
 - **Devices** - View an individual dashboard for an AP or switch. For APs, you can see associated sites, networks, clients, event logs, and traces. For switches, you can see associated ports, LAG ports, networks, event logs, and traces.
 - **Networks** - View an individual networks dashboard and associated sites, access points, switches, and clients.

- **Clients** - Blacklist or whitelist a client, and view the associated dashboard, sites, networks, and event logs.
- **Roles** - View an individual dashboard for a role and a summary.
- **Configuration** - Provides navigation to configure the following items:
 - **Sites** - Configure network segmentation, typically based on geographical location, common configuration and RF management.
 - **Networks** - Configure networks services that bind a wireless LAN service to a role. This can include rules, secure authentication options, and captive portal.
 - **Devices** - Configure switches, access points, and MLAGs. Access CLI-Mode GUI for switches. View data for all devices, unsanctioned APs, and topologies.
 - **Clients** - Whitelist and blacklist clients.
 - **Policy** - Configure policies for roles, rules, Class of Service, VLANs, VLAN groups, rates, and captive portal.
- **Tools** - Provides navigation to tools such as Port Manager, ping/trace, wireless debug, and packet capture.
- **Reports** - Provides navigation to security reports, PCI compliance reports, and audit logs.
- **Administration** - Manage accounts, system configuration.

The user menu is located in the top right corner of the screen. From left to right there are three icons followed by your user name with a drop-down menu, described in order as follows:

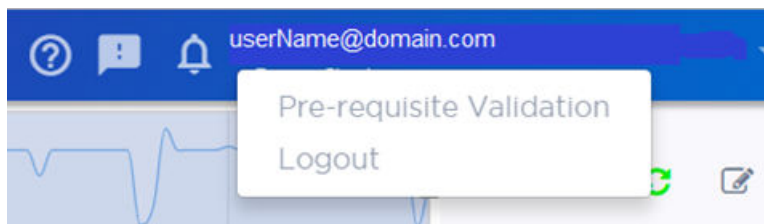


Figure 13: User Menu

- **Online Help** - The question mark icon provides context-sensitive online help.
- **Feedback** - The caption icon provides a feedback form.
- **Notifications** - The bell icon provides a list of notifications, if there are any, such as a list of unassigned switch license vouchers and entitlement expiry notices (90 days in advance).
- **Prerequisite Validation** - Select your username to open the drop-down menu and access the prerequisite validation option to assist with deployment of devices.
- **Logout** - Select your username to open the drop-down menu and log out of this application.

User Interface Changes

The user interface design separates configuration and monitoring at the parent level of the menu. This supports quick access to your preferred starting point.

The **Monitor** menu option shows the entity dashboard and displays a **Configuration** button that takes you to the **Configuration** page for that entity. This is the same underlying functionality found in previous releases. No other changes have been made to the management relationships.

The **Configuration** menu option takes you directly to configuration without displaying monitoring information.

Additional navigation changes have been made from previous releases, which are mapped in the following table:

Table 8: Mapping From Release 4.31.01 to 4.41.01

Release 4.31.01	Release 4.41.01
Clients Policy	Monitor > Clients
Policy	Configure > Policy
Sites or Devices > <i>deviceName</i> > Tools	Tools
Settings > Audit Logs	Reports > Audit Logs
Settings > Accounts	Administration > Accounts
Settings > General	Administration > General
Devices > Ports	Tools > Ports

6 Dashboard

Statistics and Intervals Configure the Dashboards

The overview **Dashboard** gives a holistic view of your sites. There are also dashboards available at the entity level for specific information about individual devices, roles, and so on.

When you log in, the overview dashboard displays by default. Navigate to this dashboard at any time by selecting **Dashboard** from the left menu.

The overview dashboard displays widgets with system level data and dashboard controls.

The Widgets

The dashboard widgets help you proactively monitor your network or troubleshoot an issue, and display data at the system level. (There are also widgets available for the [entity level](#) dashboards.) The dashboard's physical layout is [customizable and configurable](#).

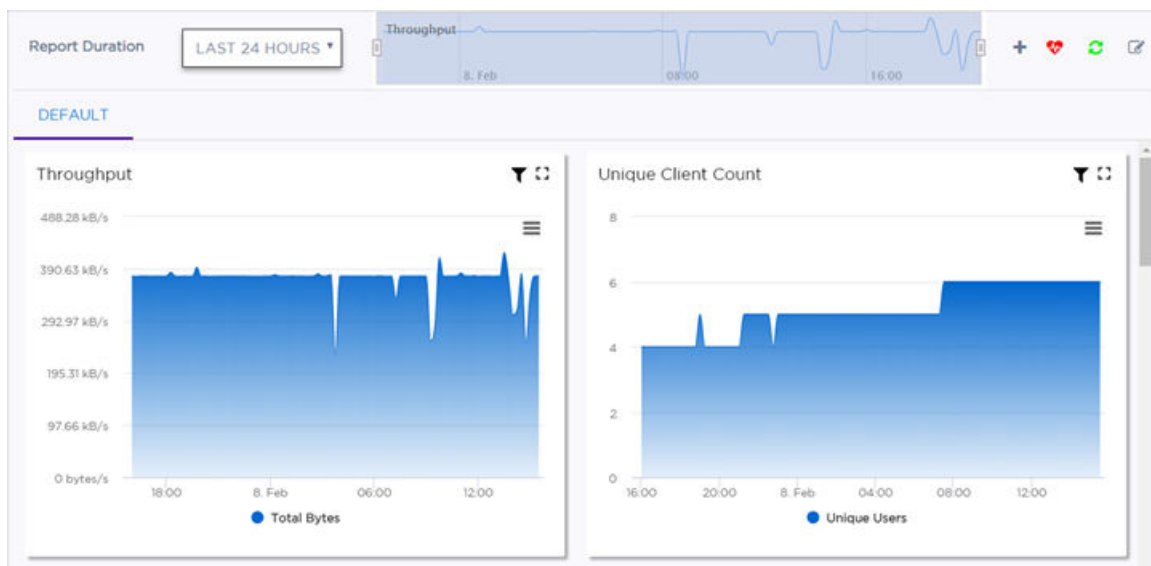


Figure 14: Dashboard

The default dashboard displays the following widgets:

- Throughput
- Unique Client Count
- Top Access Points by Throughput
- Top Access Points by Client Count

- Top Networks by Throughput
- Top Clients by Throughput
- Top Operating Systems by Client Count
- Top Application Groups by Client Count
- Top Application Groups by Throughput
- Top Switches by Throughput

Summary data values greater than or equal to ten thousand (10,000) are displayed with the suffix **K**. For example, if the actual value is 11,215, then the displayed value will be 11.21K. Similarly, the widgets display a value with the suffix **M** for values over a million (1,000,000).

Use the dashboard widgets to determine where you need to access more detailed information. For example, looking at top access points by throughput, select a specific AP in the list at the bottom of the widget. The chart information will change to show the throughput for the selected AP, and the name of the AP turns gray. Select the AP again to display the information for all of the top access points (and the name of the selected AP turns black again). Use the widget controls to filter the widget, print data, and change the viewing size.

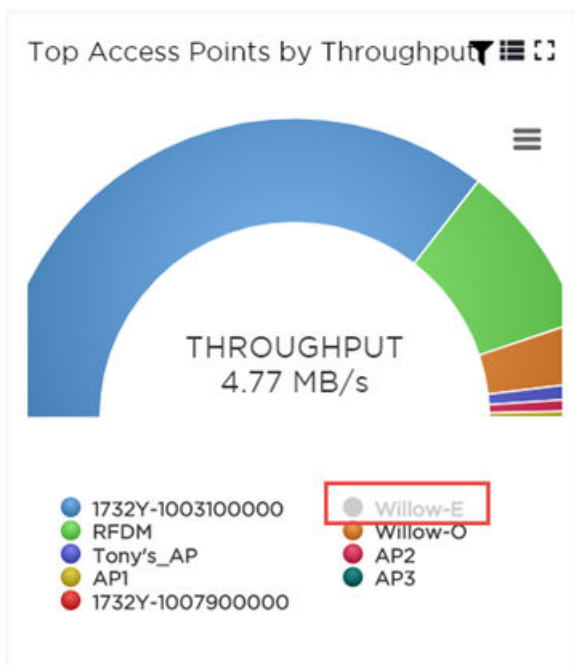


Figure 15: Example of Widget




The dashboard widgets are classified according to the data they access. Categories include Utilization, Radio Frequency (RF), Switch, Clients, Captive Portal, and Application Visibility. Widgets from any of the categories can be combined to customize the dashboard layout.

Multiple dashboards can be created with different layout and widgets. A maximum of 32 dashboards can be created per customer account.

Widget Controls

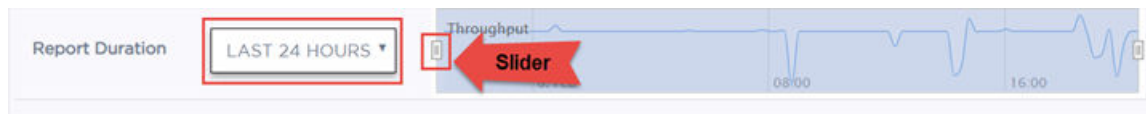
Filter the data or change the view of a widget using the controls located in the top right of each widget. Not all controls are available for each widget. The following table describes the widget controls:

Table 9: Widget Controls

Widget Control	Description
	Enables the radio band filter on each chart. Then select the radio band to filter on: All, 2.4 GHz, or 5.0 GHz.
	Enables sizing on each chart. Then select the same icon on any chart that you want to expand or reduce.
	Lets you toggle between displaying the data as a grid, a graph, or both. Not available for all charts.

Report Duration

The dashboard widgets let you filter data based on time duration. Select the report duration from the drop-down menu or use the slider at the top of the dashboard page.

**Figure 16: Report Duration**

The values in the drop-down menu are:

- Last 8 Hours
- Last 24 Hours
- Last 7 Days
- Last 31 Days

Dashboard Controls

You can see which devices are in critical, in service, and in trouble states by doing the following actions:

- 1 Select the **Network Health** icon. The number of access points and switches in each state displays.
- 2 To drill down to specific device information, select a category. The specific site and device information displays.

The dashboard controls also let you add or edit a dashboard, and refresh the view.

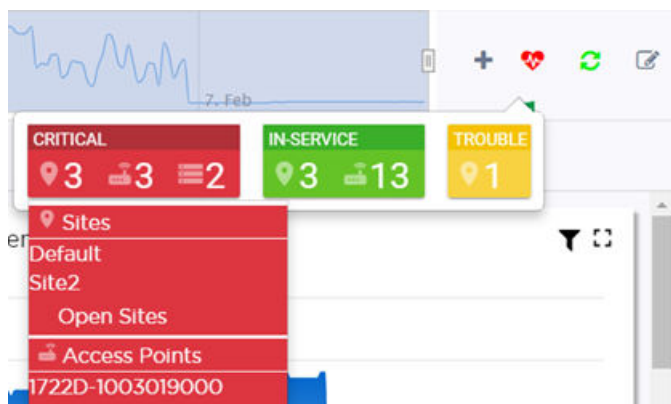




**Figure 17: Network Health Pane and Dashboard Controls**

Table 10: Dashboard Control Descriptions

Dashboard Control	Description
	Adds a customized dashboard.
	Indicates the network health. Lets you drill down to see which devices are in Critical, In Service, or Trouble states. <ul style="list-style-type: none"> • Green - The network is healthy. • Red - The network has an issue.
	Refreshes the dashboard data.
	Customizes the dashboard by adding or removing widgets.

More Information

- [Configure the Dashboards](#) on page 48
- [Statistics and Intervals](#) on page 48
- [Monitoring](#) on page 51
- [Reports](#) on page 210

Statistics and Intervals

The statistics are rolled up in 15-minute intervals, with eight hours, one day, one week, and one month durations.

Change the duration and frequency of how the data displays by selecting values from the drop-down lists in the upper right corner of the window.

Configure the Dashboards

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

To customize any dashboard:

- 1 From the main **Dashboard** page or from the [dashboard page of a specific entity](#), such as a switch or site, select .

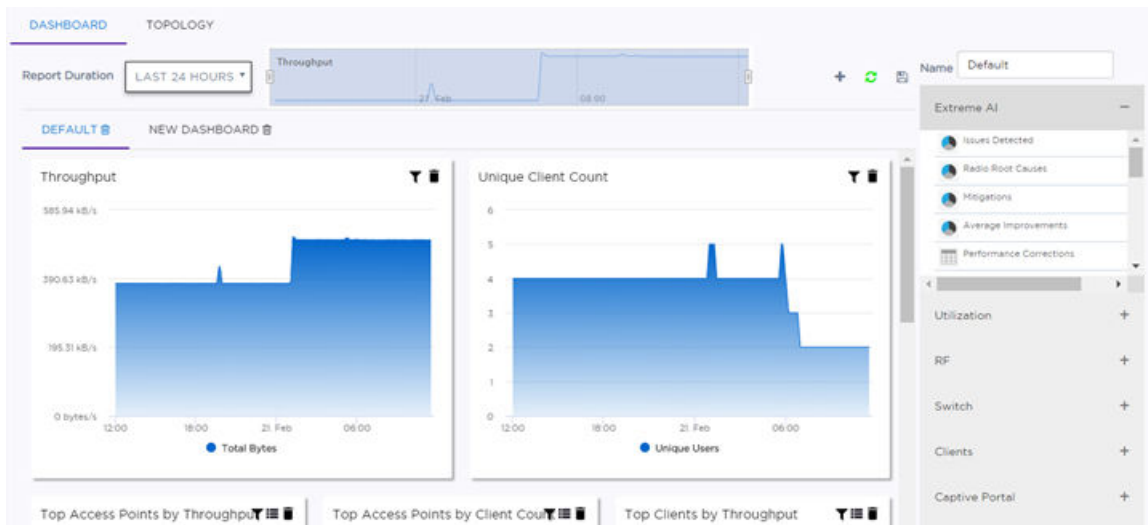


Figure 18: Dashboard - Edit Mode

The **Widgets** list displays on the right side of the page.

- 2 Expand the widget categories. Drag and drop the widgets to the placement you want in the dashboard layout. Depending on which entity dashboard (or main dashboard) you are editing, 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 metrics regarding associated guests and the amount of time guests spend using the service.
Application Visibility	Provides application visibility metrics.

- 3 (Optional) To name the dashboard, enter a name for the dashboard in the **Name** field (above the widget menu).

- 4 From the dashboard controls in the upper right corner, select the **Save Dashboard** (📄) button.

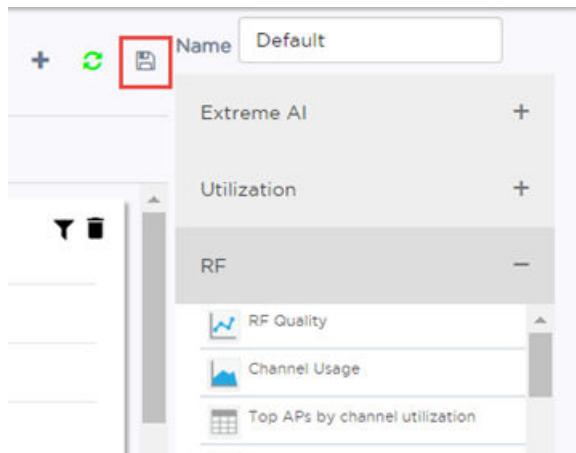


Figure 19: Save Dashboard Button

The customized dashboard is saved.

7 Monitoring

Logging
Use Topology Manager
Monitor Sites
Monitor Networks
Monitor Access Points
Monitor Switches
Monitor Clients
Monitor Roles
Monitor Applications
Monitor Unsanctioned APs for ExtremeWireless WiNG

The options for monitoring your network include:

- [Event logs](#)
- [Topology Manager](#)
- Unsanctioned AP lists and widgets for ExtremeWireless WiNG access points
- Entity dashboards and widgets

A series of entity widgets are available from the individual **Dashboard** page for each site, network, access point, switch, client, and role to give you an overall picture of the health of a specific entity.

Entity dashboards are customizable. For more information, see [Configure the Dashboards](#) on page 48.

More Information

- [Monitor Sites](#) on page 57
- [Monitor Networks](#) on page 59
- [Monitor Access Points](#) on page 60
- [Monitor Switches](#) on page 62
- [Monitor Clients](#) on page 64
- [Monitor Roles](#) on page 67
- [Monitor Applications](#) on page 68
- [Monitor Unsanctioned APs for ExtremeWireless WiNG](#) on page 69
- [#unique_77](#)

Logging

The following log files are available for event monitoring. Select a link to learn how to view the log files:

- [Event logs for sites](#)

- [Event logs for access points](#)
- [Event logs for switches](#)

[Audit log files](#) for configuration changes are located under the **Administration** menu.

View Event Logs for Sites

You can view and filter on event logs for sites and download legacy logs to see system log information about access points that are assigned to the site and clients. The live log of events on the tenant's network provides detailed insight into incidents and errors that occur on a particular network.

You can customize access and filter on the various criteria to better understand and troubleshoot the network. You can filter on severity, client information (such as 802.11 access and captive portal), and access point information (such as Smart RF and WIPS).

To view event logs for a site:

- 1 Select **Monitoring > Sites** from the menu.
- 2 Select a site from the list that displays.
The site's details page opens.
- 3 Select the **Logs** tab.
The **Events** window opens.
- 4 Select and deselect the filter criteria and time range for the events that you want to review. Selected criteria will be included in the results.

The screenshot shows the 'EVENTS' window in the monitoring interface. It includes a navigation bar with tabs: DASHBOARD, FLOOR PLANS, TOPOLOGY, NETWORKS, ACCESS POINTS, SWITCHES, CLIENTS, and LOGS. Below the navigation bar, there are filters for Start Date (02/21/2019) and End Date (02/21/2019). The Severity filter is checked for Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The Clients filter is checked for 802.11, Authentication, Roaming, and Captive Portal. The Access Point filter is checked for SmartRF, WIPS, Adoption, System, VPN, DFS, and CH Incidents. There are 'SEARCH' and 'RESET' buttons. The table below shows event logs with columns: Event Time, Event Name, Device MAC Address, Client MAC Address, Severity, and Event Message. The table contains four rows of data, including 'Radio_NoiseThreshol...' and 'Noise clear' events.


Event Time	Event Name	Device MAC Address	Client MAC Address	Severity	Event Message
2019-02-21 13:17	Radio_NoiseThreshol...	B4:2D:56:25:C3:00		info	DCS Measured Noise -80dBm Exceeded Threshold of -80dBm on
2019-02-21 13:17	Noise clear			info	Clearing due to timeout: Ap reported noise active reported for
2019-02-21 13:12	Radio_NoiseThreshol...	B4:2D:56:25:C3:00		info	DCS Measured Noise -80dBm Exceeded Threshold of -80dBm on
2019-02-21 13:12	Noise clear			info	Clearing due to timeout: Ap reported noise active reported for

Figure 20: Event Log Filtering for a Site

- Severity** (Optional) Select or deselect Severity filters: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.
- Clients** (Optional) Select or deselect Client filters: 802.11, Authentication, Roaming, Captive Portal.
- Access Point** (Optional) Select or deselect Access Point filters: Smart RF, WIPS, Adoption, System, VPN, DFS, CH Incidents.

- 5 Select **Search**.

The results display in the list below the filters. Results include event time, event name, device MAC address, client MAC address (if applicable), severity, and event message.

- 6 (Optional) Select  to export data and manage which columns display.
- 7 (Optional) Select **Reset** to reset the filter criteria to default values.

View Event Logs for APs

You can view and filter on event logs for an individual access points (APs) and download legacy logs. The live log of events on the tenant's network provides detailed insight into incidents and errors that occur on a particular network. You can also customize access and filter on the various criteria to better understand and troubleshoot the network.

The event history includes all Smart RF related events including radios being added, channel and power changes as well as Neighbor Recovery, Interference Recovery and Coverage Hole Recovery events.

To view event logs for an individual AP:

- 1 Select **Monitor > Devices > Access Points** from the menu.
- 2 Select an access point from the list that displays.
The access point's details page opens.
- 3 Select the **Event Logs** tab.
- 4 Select and deselect the filter criteria and time range for the events that you want to review. Selected criteria will be included in the results.

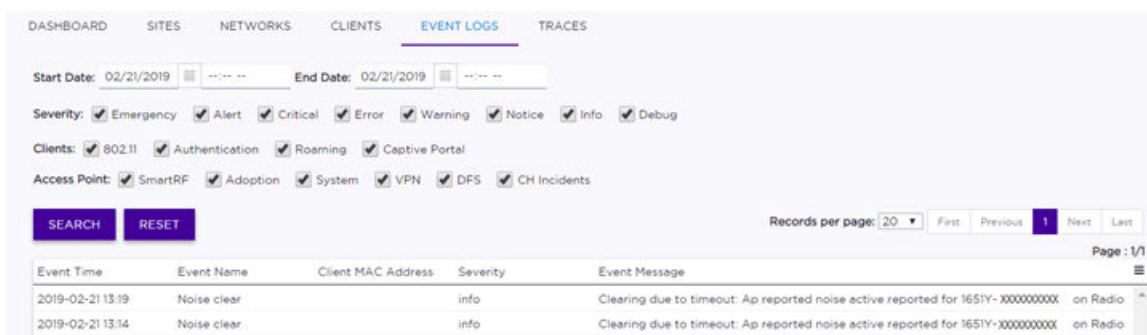



Figure 21: Event Log Filtering for an AP

- Severity** (Optional) Select or deselect Severity filters: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.
- Clients** (Optional) Select or deselect Client filters: 802.11, Authentication, Roaming, Captive Portal.
- Access Point** (Optional) Select or deselect Access Point filters: Smart RF, WIPS, Adoption, System, VPN, DFS, CH Incidents.

- 5 Select **Search**.
The results display in the **Event Logs** list below the filters. Results include event time, event name, client MAC address (if applicable), severity, and event message.
- 6 (Optional) Select  to export data and manage which columns display.
- 7 (Optional) Select **Reset** to reset the filter criteria to default values.

View Event Logs for Switches

You can view and filter on event logs for individual switches and download legacy logs. The live log of events on the tenant's network provides detailed insight into incidents and errors that occur on a particular network. You can also customize access and filter on the various criteria to better understand and troubleshoot the network.

To view event logs for a switch:

- 1 Select **Monitor** > **Devices** > **Switches** from the menu.
- 2 Select a switch from the list that displays.
The switch's details page opens.
- 3 Select the **Event Logs** tab.
- 4 Select and deselect the filter criteria (by severity type) and time range for the events that you want to review. Selected criteria will be included in the results.

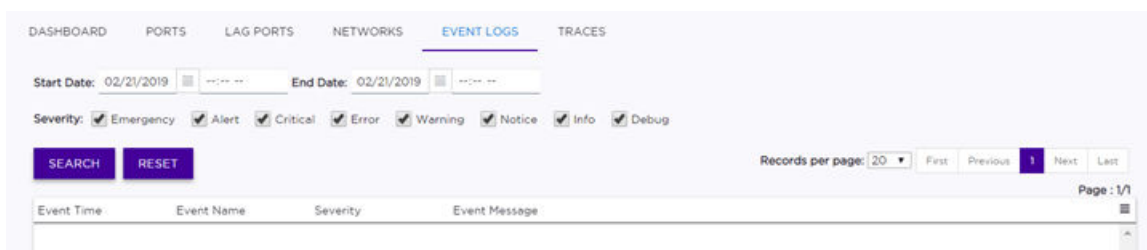



Figure 22: Event Log Filtering for a Switch

- 5 Select **Search**.
The results display in the **Event Logs** list below the filters. Results include the event time, event name, severity, and event message.
- 6 (Optional) Select  to export data and manage which columns display.
- 7 (Optional) Select **Reset** to reset the filter criteria to default values.

Use Topology Manager

Topology Manager monitors the network topology state for physical devices, showing L2 switch interconnects and the end device connections to the switch. The data is displayed in the user interface using a physical layer diagram to show a switch and what is connected to each port. Zoom in and out to see the state of nodes and edge devices in a network.

To access and use the Topology Manager:

- 1 Select **Monitor > Sites**. Select a site from the list, and select the **Topology** tab. The **Topology** page displays.

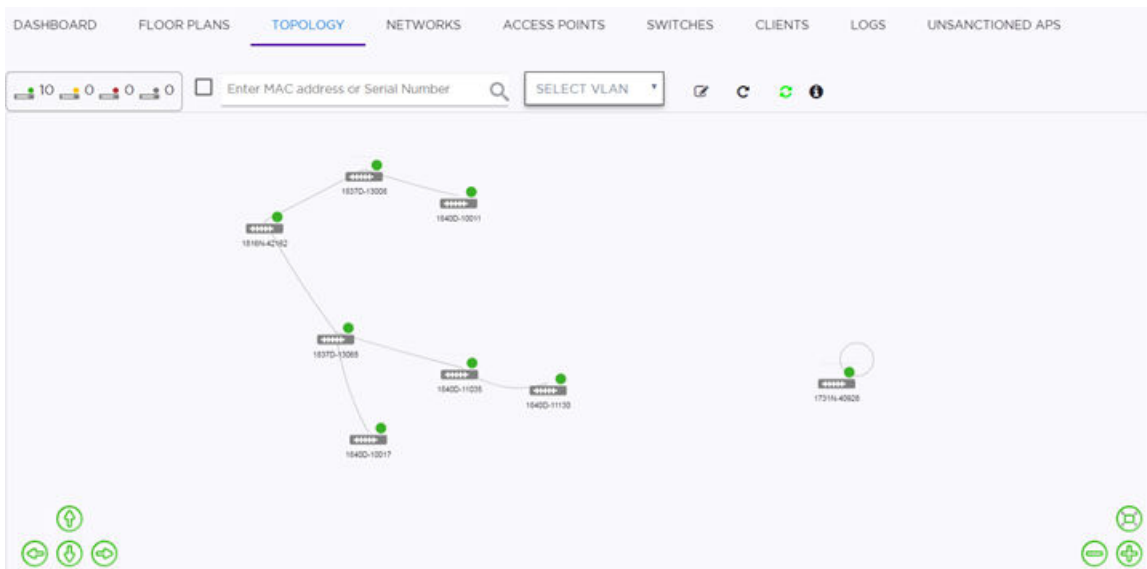


Figure 23: Topology Manager - Site View

- 2 Use the menu at the top to filter by or display specific criteria:

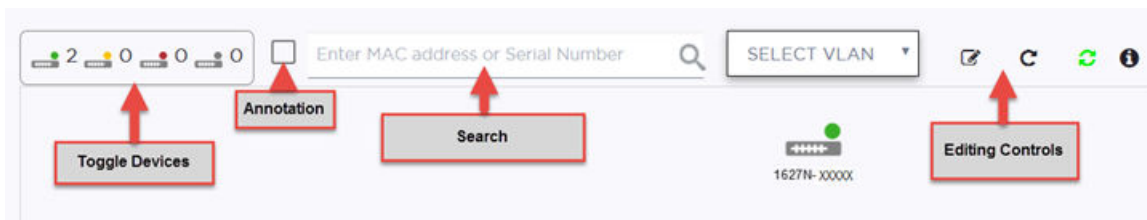


Figure 24: Topology Menu

Toggle Devices A graphic box displays a set of switches in different states, showing the number of switches in each state. Select the graphic box to toggle to a set of access points that show the number of access points in each state. The states are:

- **Green** - In service
- **Yellow** - Trouble
- **Red** - Critical
- **Gray** - Unknown

Annotation By default, the **Annotation** checkbox is disabled. Select the checkbox to display the ports on the edge between devices in the topology diagram.

Search Search by MAC address or by devices serial number.

Select VLAN If available, select a VLAN to filter on in the current nodes that display. You can use this option at any level of the topology, such as site, switch, access point, or client.

Editing Controls Lets you edit, save, undo, redo, and regenerate the map. To edit the nodes (icons), select **Edit**, then drag the nodes and select **Save**. The **Refresh** button refreshes the page.

- 3 To view the APs, select **+** in the bottom right corner or use your mouse wheel to zoom in.

- (Optional) Select a device to display the device details, such as hardware type, serial number, and port information.

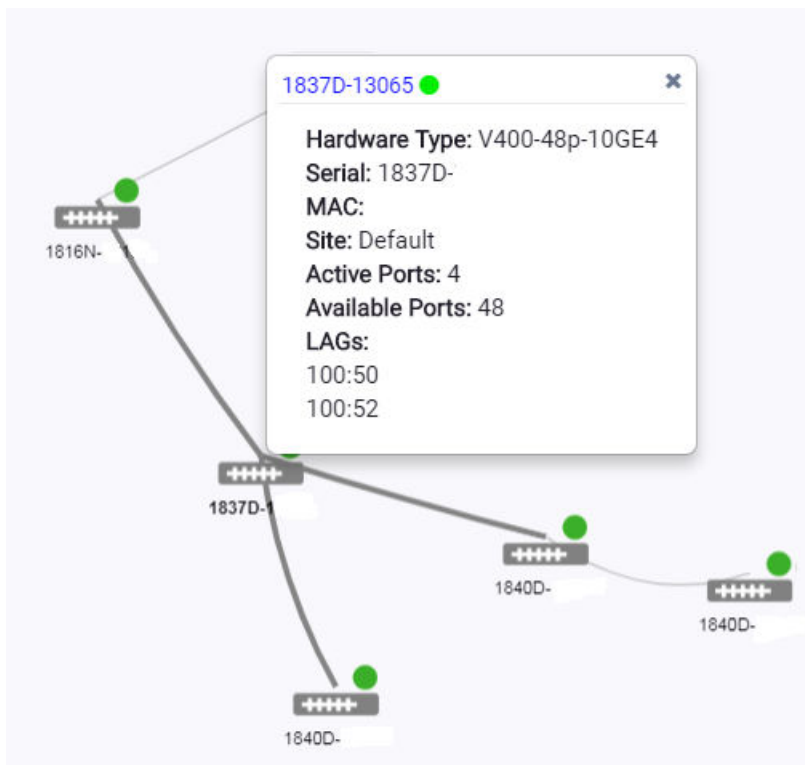


Figure 25: Device Details

- (Optional) Select the edge of a device to see detailed information about the links, such as ports, speed, and STP state.

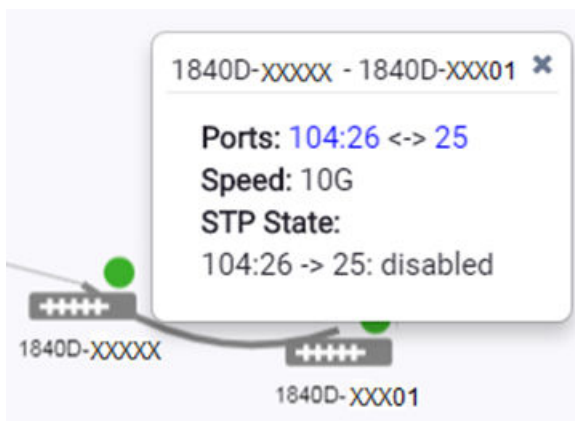


Figure 26: Link Information

- 6 (Optional) Select a VLAN from the menu.

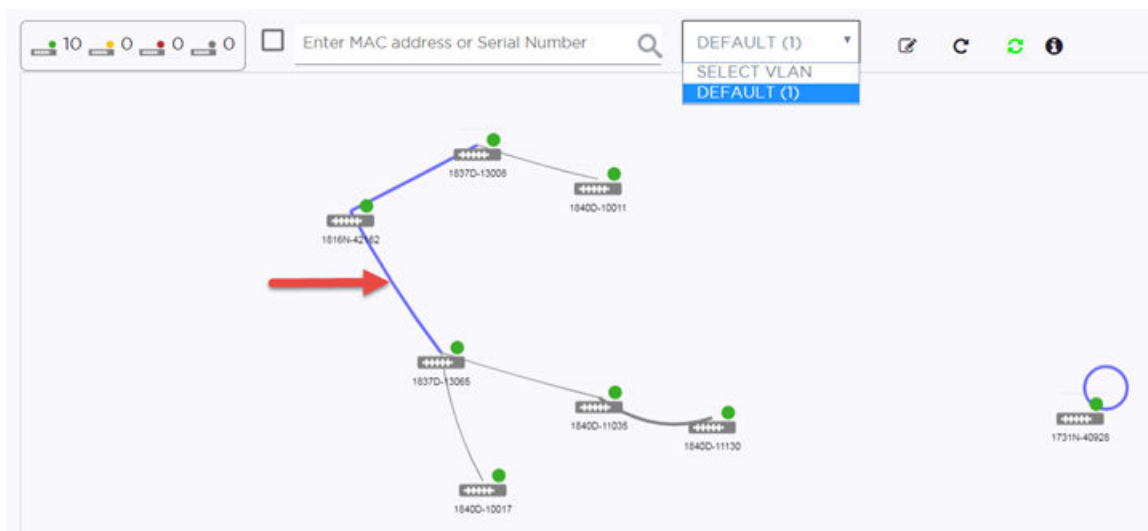


Figure 27: VLAN Links

The paths between the devices are highlighted in purple.

- 7 (Optional) To add a client to the map, search for the client's MAC address using the **Search** field. The client is added to the map with corresponding client type type.

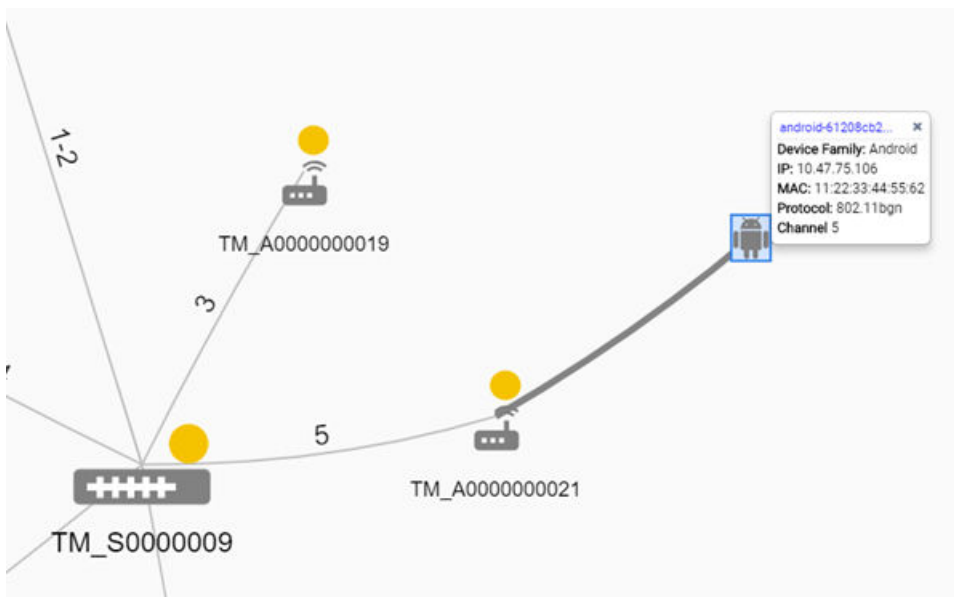


Figure 28: Client MAC Details

- 8 (Optional) To see a device (or client) statistics page, select the corresponding icon in the map.

Monitor Sites

The **Monitor > Sites** page shows all of your sites. Do any of the following actions:

- View a list of all sites using either the **Grid** or **List** tab.
- Search for a site using the **Search** field.
- View or edit the entity dashboard.
- On a site page, select the tabs to access information about the associated floor plans, topology, networks, access points, switches, clients, logs, and unsanctioned APs.

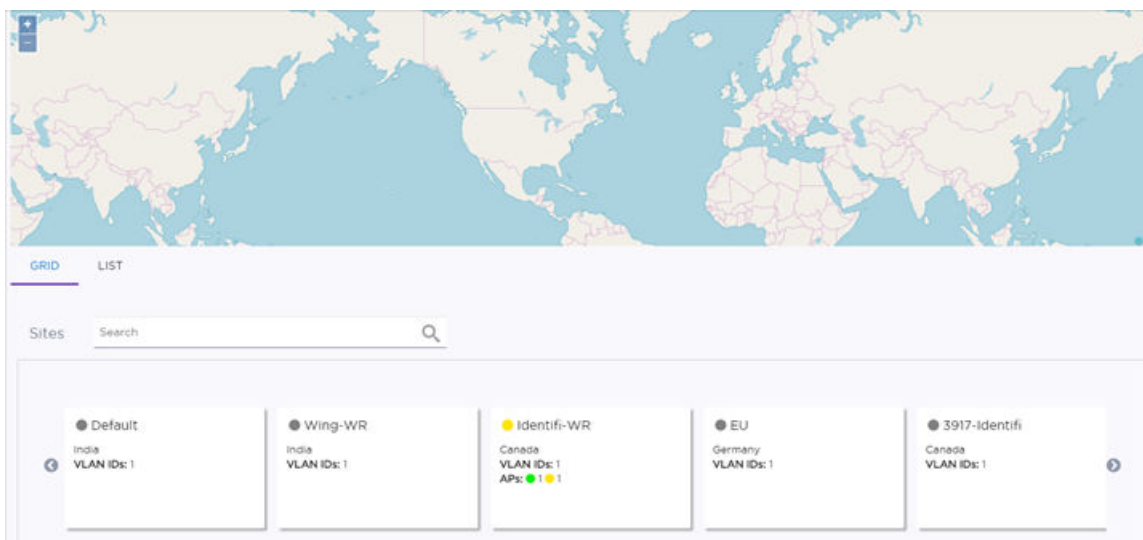


Figure 29: Monitor Sites Page

Depending on the tab you select, you can manage, configure, filter, or perform other actions, such as:

Floor Plans	Manage device placement and view heat maps, channels, link speed, and RFQI. Toggle between 5 GHz and 2.4 GHz radios. Add or remove badges.
Topology	View the site topology and drill down to see links between ports.
Networks	See the list of associated networks. Select a network to open the configuration page.
Access Points	See the list of associated access points. Select an access point to open the configuration page.
Switches	See the list of associated switches. Select a switch to open the configuration page.
Clients	See a list of associated clients. Select a client to blacklist or whitelist the client.
Logs	View and filter the list of event logs.
Unsanctioned APs	If the site is an ExtremeWireless WiNG site, any unsanctioned APs are listed. You can filter the list.

On the individual site **Dashboard** page, widgets show historical data that can help you determine a baseline and identify unusual activity.

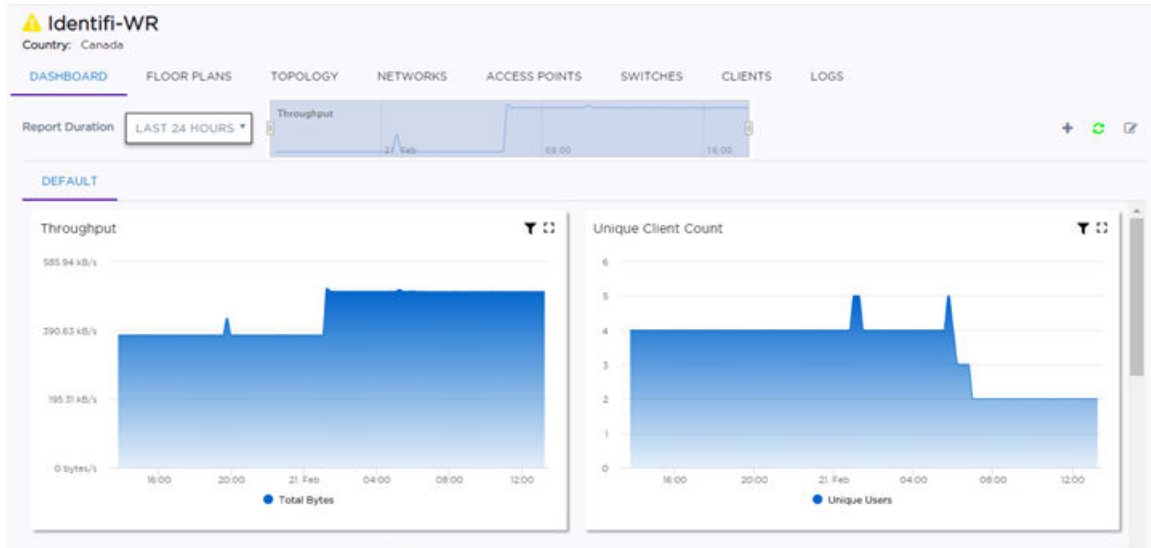


Figure 30: Individual Site Dashboard

The dashboard can be customized to use other available widgets. For example, these widgets can include the following information:

- List of services provided by the site
- Total site usage over time
- Distribution of device/OS types
- Busiest APs and busiest switches in the site during a sliding window of a fixed number of days
- Busiest users of the site during a sliding window of a fixed number of days
- Device identification for top manufacturers and top operating systems by client

More Information

- [Configure the Dashboards](#) on page 48
- [Monitoring](#) on page 51

Monitor Networks

The **Monitor > Networks** page shows a list of all of your networks.

Name	SSID	Status	Default Role	Privacy Type	Default VLAN
Staff	Staff	Enabled	Allow all	WPAv2 with PSK	Default
Wing-441	Wing-441	Enabled	Allow all	WPAv2 with PSK	Default
Identifi-441	Identifi-441	Enabled	Allow all	WPAv2 with PSK	Default
identifi-open-441	identifi-open-441	Enabled	Allow all	Open	Default

Figure 31: Monitor Networks Page

Do any of the following actions:

- Search for a network using the **Search** field.
- Select a network to open the network page and view the information for that entity. The entity dashboard displays by default.

- Select the tabs to access information about the associated sites, access points, switches, clients.

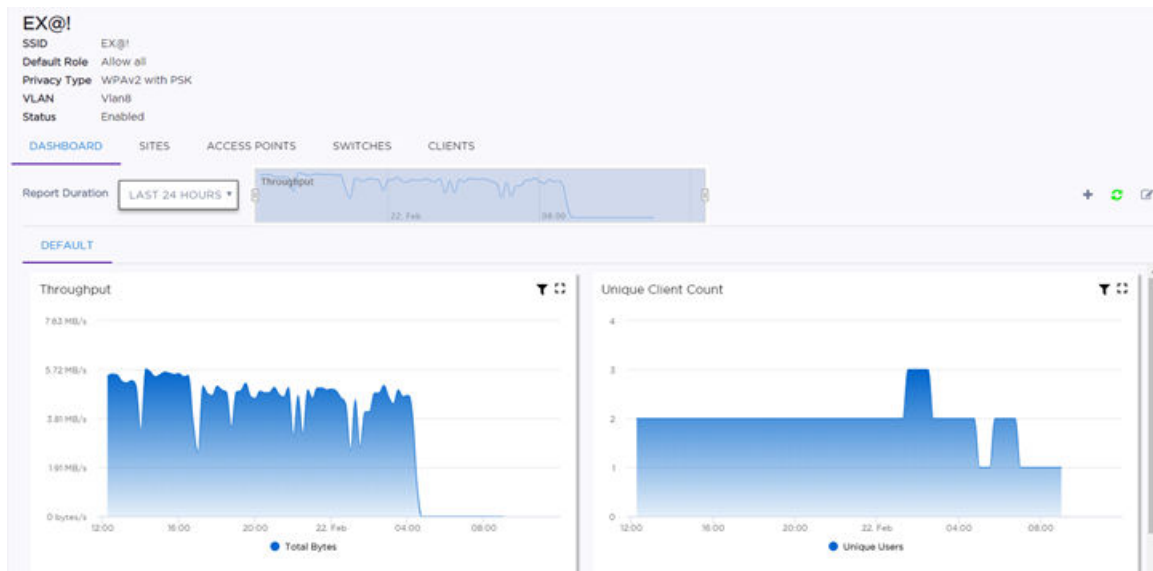


Figure 32: Individual Network Dashboard

Depending on the tab you select, you can manage, configure, filter, or perform other actions, such as:

- Sites** View the list of associated sites. Select a site to open the configuration page.
- Access Points** View the list of associated access points. Select an access point to open the configuration page.
- Switches** View the list of associated switches. Select a switch to open the configuration page.
- Clients** View a list of associated clients. Select a client to blacklist or whitelist the client.

On the individual network **Dashboard** page, widgets show historical data that can help you determine a baseline and identify unusual activity.

These widgets provide information about usage patterns specific to an individual configured SSID/network. (Services include the type of wireless security, privacy filters, and RADIUS servers used, if any.) This information helps you to plan for scaling the network. Understanding the distribution of device types on the network can help to identify ancillary services that should be provided. For example, if the network has a high percentage of IOS devices, you may choose to enable Bonjour traffic controls.


The dashboard can be customized to use other available widgets, such as the distribution of device/OS types and applications over a period of time.

More Information

- [Monitoring](#) on page 51
- [Configure the Dashboards](#) on page 48

Monitor Access Points

The **Monitor > Devices > Access Points** page shows a list of your access points. Do any of the following actions:

- Adjust the number of records that display per page.
- Use the menu icon () to adjust which columns display and to export data to CSV.
- Search for an access point using the **Search** field.
- Select an access point and view the details that display. If there is an associated floor plan, it displays in the top right corner. Select the floor plan to access the floor plan tools, such as viewing heat maps.
- View or edit the entity dashboard. The statistical details can be configured, such as time range.
- On an access point page, select the tabs to access information about the associated sites, networks, clients, event logs, and traces.
- Select the link at the top to troubleshoot connectivity issues.

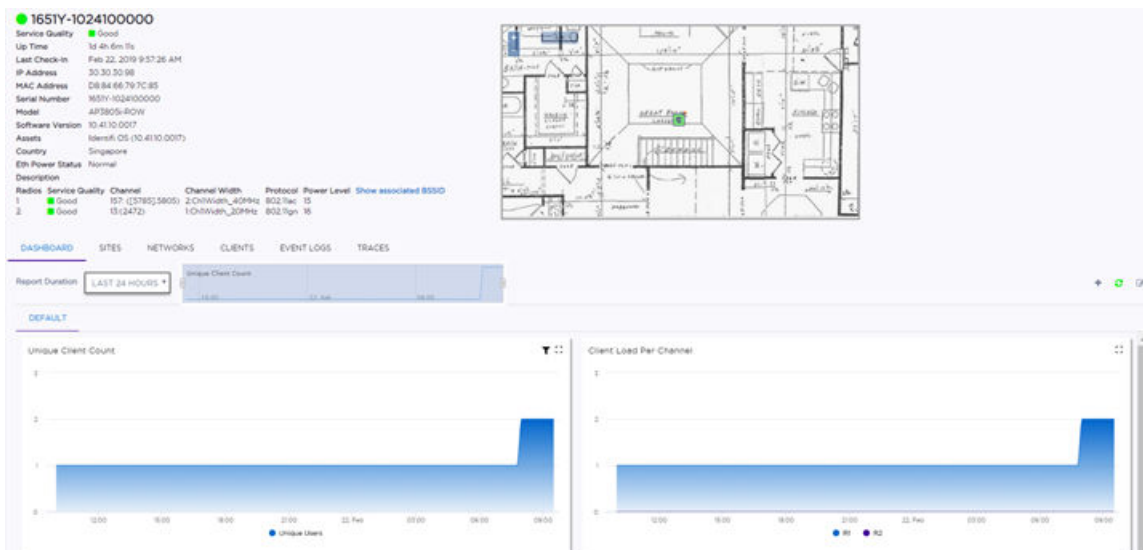




Figure 33: Individual Access Point Dashboard

Depending on the tab you select, you can manage, configure, filter, or perform other actions, such as:

- Sites** View the list of associated sites. Select a site to open the configuration page.
- Networks** See the list of associated networks. Select a network to open the configuration page.
- Clients** View a list of associated clients. Select a client to blacklist or whitelist the client.
- Event Logs** View the list of event logs. Search for an event or filter the list. Data can be exported using the menu icon () .
- Traces** View traces.

Each device has its own dashboard. These entity widgets provide basic information for an individual AP device, including device type, MAC address, serial number, entitlement status, model name, port status, site, and management IP address on the LAN.

Select the Edit Dashboard () icon to configure which widgets display. For example, these widgets can include the following information:

- Last reported 2.4 GHz and 5.0 GHz channels, including channel width
- Percent of channel utilization over time
- Usage in number of bytes, packets, and users over time
- Total usage by service/SSID (Top Services by Throughput) and radio (Channel Utilization)

- Radio noise levels in dBm
- Device identification for top manufacturers and top operating systems by client
- Application visibility

Widgets for wired client ports include:

- Throughput
- Unique client count
- Utilization errors
- Discarded packets

All AP widgets are available for all model types, with the exception of the following widgets:

Table 11: Model-Specific AP Widgets

Widget Name	Applies To
Top App Groups By Throughput Report	ExtremeWireless only
Top App Groups By Client Count Report	ExtremeWireless only
Top Apps By Throughput Report	ExtremeWireless WiNG only
Worst Apps By Throughput Report	ExtremeWireless WiNG only
Top Apps By Unique Users	ExtremeWireless WiNG only
Smart RF History	ExtremeWireless WiNG only
Top APs By Channel Changes	ExtremeWireless WiNG only
Top APs By Power Changes	ExtremeWireless WiNG only
Top APs By Coverage Hole Changes	ExtremeWireless WiNG only
Top Sites By Channel Changes	ExtremeWireless WiNG only
Top Sites By Power Changes	ExtremeWireless WiNG only
Top Sites By Coverage Hole Changes	ExtremeWireless WiNG only
Guest Users Report	ExtremeWireless WiNG only
Dwell Time Report	ExtremeWireless WiNG only

More Information

- [Monitoring](#) on page 51
- [Configure the Dashboards](#) on page 48

Monitor Switches

The **Monitor > Devices > Switches** page shows a list of your switches.

Status	Name	Serial Number	Description	IP Address	Site	Version	Model
●	1602N-XXXX	1602N-XXXX			Default		X620-16x-Base
●	1603N-XXXX	1603N-XXXX			Default		X440-G2-12t-10GE4
●	1612N-XXXX	1612N-XXXX			Default		X440-G2-48t-10G...
●	1628N-XXXX	1628N-XXXX			Default		X440-G2-24p-10G...
■	1729N-XXXX	1729N-XXXX			Default		220-48p-10GE4
■	1730N-XXXX	1730N-XXXX			Default		210-12t-GE2

Figure 34: Monitor Switches List

Do any of the following actions:

- Adjust the number of records that display per page.
- Use the menu icon (☰) to adjust which columns display and to export data to CSV.
- Search for a switch using the **Search** field.
- On an individual switch page, view the details that display, including hardware information about power supplies, power budget, fans and temperature.
- View or edit the entity dashboard.
- On a switch page, select the tabs to access information about the associated ports, LAG ports, networks, event logs, and traces. If an Extended Edge Switch is in the controlling bridge role, a **Port Extenders** tab appears and displays information about switches that are serving as bridge port extenders (BPEs).
- Configure the switch.

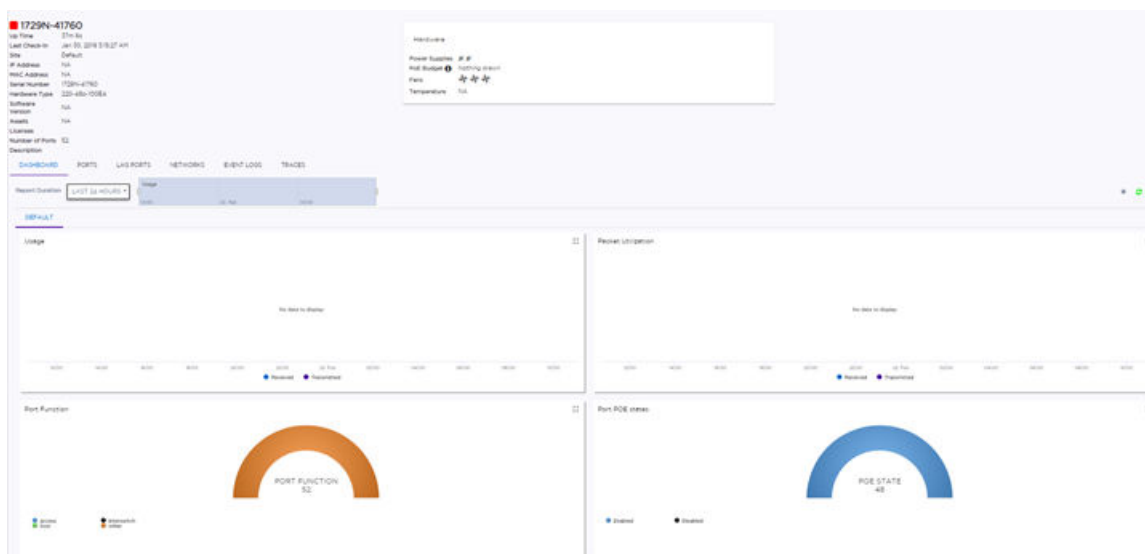


Figure 35: Switch Dashboard

Depending on the tab you select, you can manage, configure, filter, or perform other actions, such as:

- Ports** View the details of the associated ports, such as link state, admin state, name, alias, function, port speed, and neighbor. Data can be exported to CSV using the menu icon (☰).
- LAG ports** View the details of any associated Masters and LAG members. Data can be exported to CSV using the menu icon (☰).
- Networks** See the list of associated networks. Select a network to open the configuration page.

Event Logs View the list of event logs. Search for an event or filter the list. Data can be exported to CSV using the menu icon (☰).

Traces View traces.

Each switch has its own dashboard, which can be customized. 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 4 possible port functions:
 - Serve an Access Point
 - Serve a Host (other than an access point)
 - Link to another bridge/switch
 - Other
- Port PoE states

More Information

- [Monitoring](#) on page 51
- [Configure the Dashboards](#) on page 48

View Switch Traces

You can view traces for an individual switch.

- 1 Select **Configure** > **Devices** > **Switches** from the menu.
- 2 Select a switch from the list.
- 3 Select the **Traces** tab.

The **Traces** tab automatically opens for the device and you can view the trace files in the user interface.

Monitor Clients

The **Monitor** > **Clients** page lists all of the clients in the networks, their status, MAC address, IP address, and other information. Use this information to manage and troubleshoot devices, and blacklist or whitelist clients by MAC address.

Select the menu icon (☰) to see the list of options for the page. You can specify the **Refresh** option, export some or all of the data to a CSV file, and configure which data columns display. By default, all columns display.

Clients Search Exact match BLACKLIST

Sort By: MAC Address Records per page: 20 1 Page: 1/1

Status	IP Address	MAC or Hostname	Last Seen	Device Type	AP	rssi (dBm)	Site	Role	Blacklist
●	192.0.2.3	IPv6 <hostname>	Mar 19, 2018 3:02:47 PM	Unknown	1000000000000009	-50	Site4-3917	Allow all	<input 162="" 201="" 218"="" 395="" data-label="Caption" type="button" value="+</input></td> </tr> </tbody> </table> </div> <div data-bbox="/> <p>Figure 36: Clients List Page</p>

Search for a client using the **Search** field.

Blacklist a client using either the **Blacklist** button or selecting the plus icon () next to a specific client.

Select a client from the list to open the individual client's **Dashboard** page and view the statistical details. View or edit the entity dashboard.

Each client has its own dashboard, which can be customized. The widgets can include the following information:

- Current or last known site
- Current authentication status (if online) or the last time seen
- Current or last access point to which the client associated
- RSSI from the last reporting AP (if known)
- Client type (if known)
- OS type (if known)
- Currently assigned role or last assigned role
- MAC address
- Current IP address (if online)
- User name (ExtremeWireless WiNG only)
- Usage in bytes per second, recorded for up to one month, using 15-minute roll-ups
- Top applications in use by the client, based on bytes per second, identified as belonging to the application

If there is an associated floor plan, it displays in the top right corner. Select the floor plan to access the floor plan tools, such as viewing heat maps.

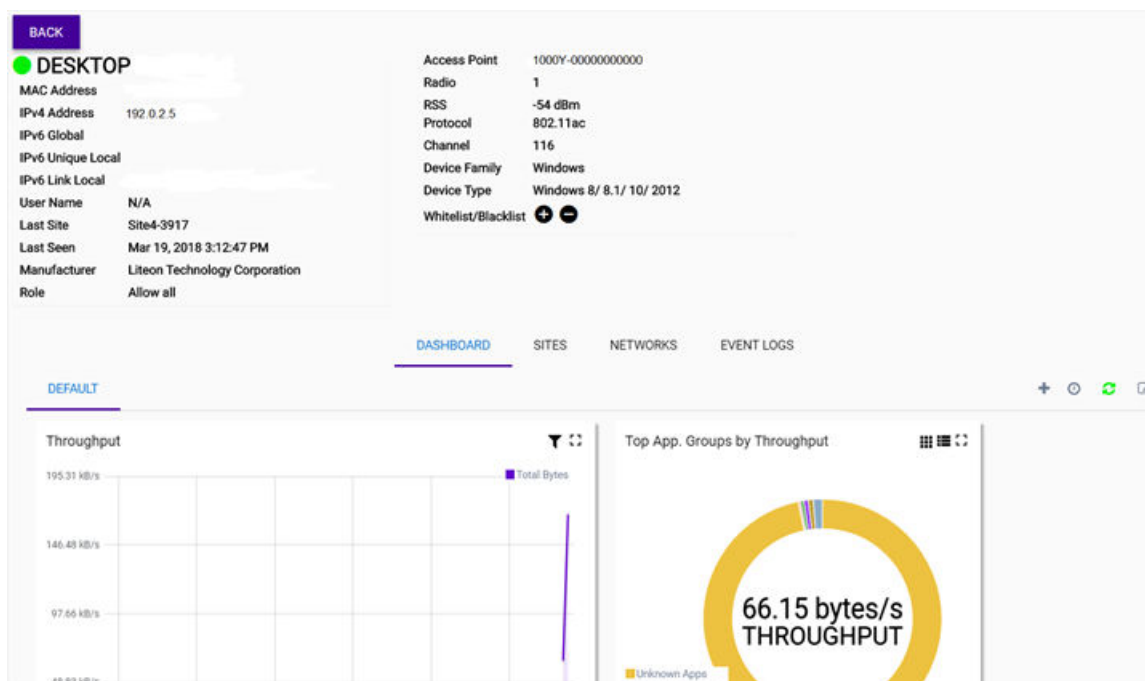


Figure 37: Individual Client Dashboard

Select the tabs to access information about the associated sites, networks, and event logs:

- Sites** View the list of associated sites. Select a site to open the configuration page.
- Networks** See the list of associated networks. Select a network to open the configuration page.
- Event Logs** View the list of event logs. Search for an event or filter the list. Data can be exported using the menu icon (☰).

More Information

- [Monitoring](#) on page 51
- [Configure the Dashboards](#) on page 48
- [Whitelist and Blacklist Clients](#) on page 66

Whitelist and Blacklist Clients

A client's MAC address is used to whitelist or blacklist the client.

- 1 Select **Monitoring > Clients** from the menu.

A list of clients displays. You can select a client in the list and either whitelist or blacklist a client from the **Client List** page. Alternatively, you can perform the rest of this procedure.

- 2 Select **Blacklist**.

The screenshot shows the 'Configure Client' interface. At the top left is a 'BACK' button. On the right are 'SAVE', 'ADD', and 'DELETE' buttons. Under the 'Mode' heading, there are two radio button options: 'Allow MAC only if on the MAC address list' and 'Deny MAC address if it is on the list'. The second option is selected. Below this is the 'MAC Addresses' section, which contains a single entry 'MAC Address' with a checkmark to its left.

Figure 38: Configure Client

The **Configure Client** page opens.

- 3 To whitelist a client, select **Allow MAC only if on the MAC address list**. To blacklist a client, select **Deny MAC address if it is on the list**.



Note

To delete a client from a whitelist or blacklist, select a MAC address from the list and select **Delete**.

- 4 Select **Add**.

The **New MAC Address** dialog opens.

New MAC Address

The screenshot shows the 'New MAC Address' dialog box. It has a title bar at the top. Below the title is a large, empty rectangular text input field with a red border. At the bottom of the dialog, there are two buttons: 'CANCEL' and 'OK'.

Figure 39: New MAC Address

- 5 Enter the client's MAC address. Select **OK**.
You return to the **Configure Client** page.
- 6 Select **Save**.

Monitor Roles

The **Monitor > Roles** page shows all of your roles.

Name	Default Action	# Rules
Allow all	allow	0
Deny all	deny	0
SampleStaff	deny	2
TypicalGuest	deny	5

Figure 40: Monitor Roles Page

Do any of the following actions:

- Search for a role using the **Search** field.
- Select a role to view or edit the entity dashboard.
- On a role page, select the **Summary** tab to view configuration details about the role, such as bandwidth limit.

Each role has its own entity dashboard. The dashboard can be customized to use other available widgets. For example, these widgets can include the following information:

- Top application groups by client count
- Top application groups by throughput

More Information

- [Monitoring](#) on page 51
- [Configure the Dashboards](#) on page 48

Monitor Applications

Application Visibility widgets are available when you [customize a dashboard](#).

To view application widgets and details:

- 1 From any dashboard, look for an application widget. Some widgets have a **Treemap view** icon.



Figure 41: Application Widget with Treemap View Icon

- 2 To see a detailed breakdown of the statistics, select the **Treemap view** icon.

More Information

- [Monitoring](#) on page 51
- [Configure the Dashboards](#) on page 48

Monitor Unsanctioned APs for ExtremeWireless WiNG

This feature is available only for ExtremeWireless WiNG access points (APs) that have WIDS enabled.

Unsanctioned (rogue) access points are devices that are detected in a sanctioned radio coverage area but have not been deployed by the network administrator as a known device. Authorized access points and clients are generally known to the administrators and conform with the organization's security policies. Unsanctioned access points should be filtered to avoid jeopardizing the data within a managed network.

To monitor unsanctioned ExtremeWireless WiNG APs:

- 1 From the menu, do **one** of the following actions:
 - To view all unsanctioned APs, select **Monitor > Devices > Unsanctioned APs**.
 - To view unsanctioned APs assigned to a site, select **Monitor > Sites**. From the **Sites** list, select an ExtremeWireless WiNG site, and select the **Unsanctioned APs** tab.)
- 2 A list of rogue and unsanctioned APs displays.

- 3 Review the list to help determine what actions your organization wants to take. Select a column heading to reorder the rows in a way that makes sense for you.

Threat Type	The classification of the AP as an unsanctioned device.
BSSID	The Basic Service Set (BSS) that the unsanctioned access point belongs to. (A BSS is a set of stations that can communicate with one another.) Select the link to view further details for this unsanctioned access point.
Security Type	The security type in use on the unsanctioned access point.
SSID	The Service Set ID (SSID) of the network to which the detected unsanctioned access point belongs.
Vendor	The manufacturer name for the unsanctioned access point.
Last Seen Channel	The last channel on which the unsanctioned access point was detected.
rssi (dBm)	The signal strength of the detected unsanctioned access point.
First Seen	The timestamp when this unsanctioned access point was first detected.
Site	The tenant-managed site where this unsanctioned access point was discovered.
Top Reporter	The user assigned name of the access point that reported this unsanctioned access point.

- 4 (Optional) Select an AP in the list and use the icons to refresh the list, reset the columns to the default order, print the information displayed in the table, or export the data.

8 How to Configure Your Network

The first administrator in your company to log in to the ExtremeCloud user interface is presented with a configuration wizard that automatically opens to complete the initial configuration. Your configuration is initialized with a default site and a service that are best used to determine initially that your new devices are functioning properly. We recommend replacing the default settings using the configuration wizard, or exiting the wizard and creating new services and roles to meet your specific needs.

To modify or configure a network manually, follow this process:

- 1 Log in to your ExtremeCloud administrator account at <https://ezcloudx.com>.
- 2 Configure the network:
 - a Configure network services, including authentication.
 - b Configure roles or policies.
 - c Configure Class of Service.
 - d Configure VLANs.
 - e (Optional) Configure advanced network settings.
- 3 Configure cloud-managed switches, if you are using them.
- 4 Configure a site and, optionally, advanced site settings.
- 5 Configure access points.

9 Configuring Sites

Configure a Site
Clone a Site
Delete a Site
System Log Configuration
How to Enable Location Analytics
SNMP
Wireless Intrusion Detection Services (WIDS)

The **Configure > Sites** page shows all of your sites. Do any of the following actions:

- View a list of all sites using either the **Grid** or **List** tab.
- Search for a site using the **Search** field.
- To edit a site, select a site from the list. The **Configuration** page opens.
- To add a new site, select **Add**.



Note

A site that contains ExtremeWireless WiNG APs will not contain ExtremeWireless APs. Also, a site will not combine ExtremeWireless WiNG 5 and 7 model access points. The configuration options that display depend on the type of APs deployed at the site.

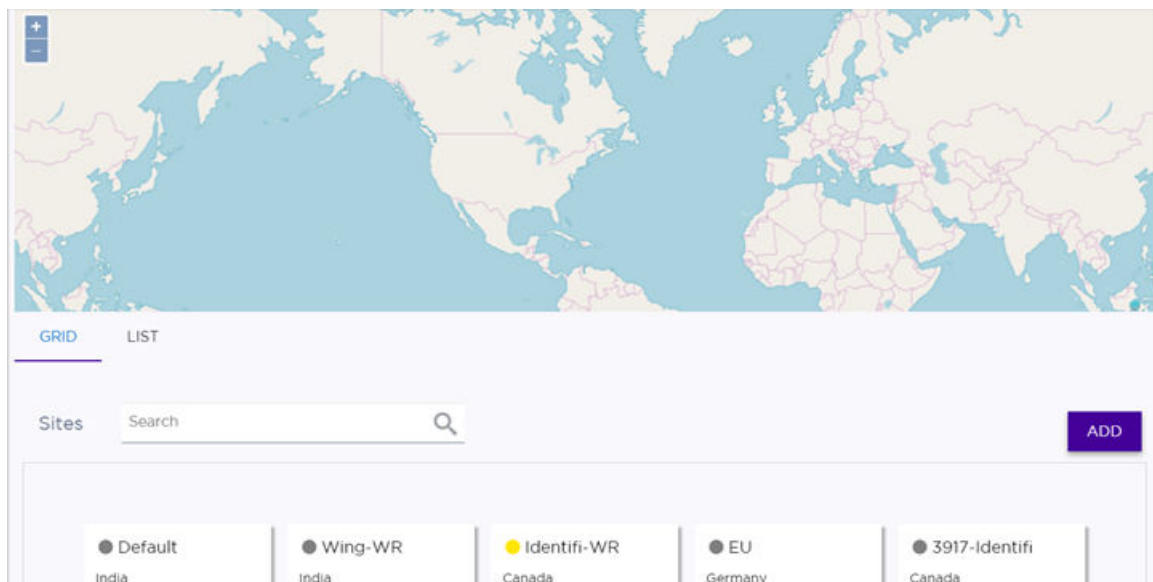


Figure 42: Configure Sites - Grid View

On the **Configure Site** page, select the tabs to access and configure information about the floor plans, location, networks, devices, roles, RF management, VLANs, advanced radio settings, advanced settings, and Internet of Things (IoT) associated with that site.

More Information

- [Configure a Site](#) on page 73
- [Clone a Site](#) on page 105
- [Delete a Site](#) on page 106
- [How to Enable Location Analytics](#) on page 106

Configure a Site

When you connect a device (switch or AP) to the cloud, the device is assigned to a default site. You can assign the device to a different site at any time. You can also add new sites and configure other aspects of existing sites.

Additionally, if you create a new network (wireless SSID), you must add the network to a site to provide the services to the wireless devices at that site.



Note

A site that contains ExtremeWireless WING APs will not contain ExtremeWireless APs. Also, a site will not combine ExtremeWireless WING 5 and 7 model access points. The configuration options that display depend on the type of APs deployed at the site.

To configure a site:

- 1 Select **Configure > Sites** from the menu.
The **Sites** list displays.
- 2 To add a new site, select **Add**. Alternatively, select an existing site, and select **Configure Site**.
The **Configure Site** page opens.

Figure 43: Configure Site Page

- 3 Enter a name for the site, country, and timezone. Every site must be assigned to a country, which determines which types of APs can be deployed at this site. A site is either FCC compliant or ROW compliant, depending on the country selected. A site that is ROW compliant can accept only AP models ending in 'ROW'. A site that is FCC compliant can accept only AP models ending in 'FCC'. The country assigned to a site has no effect on which types of switches can be added to the site.
- 4 Select each of the following tabs to configure a new site. For an existing site, select only the tabs whose configuration you want to change.
 - **Floor Plans** - Optional
 - **Location** - Optional
 - **Networks** - Required
 - **Device Adoption Rules** - Optional
 - **Devices** - Required
 - **Roles** - Optional
 - **RF Management** - Optional
 - **VLANs** - Optional
 - **Advanced Radio Settings** - Optional
 - **Advanced Settings** - Optional
 - **IoT** - Optional
 - **Air Defense Profiles** - Optional
- 5 Select **Save**.

Configure 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, but the devices represented in the map must come from the same site.



Note

There is a limit of 200 floors per site.

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 Upload a background image.
- 2 Specify the environment and scale.
- 3 Draw the boundary walls.
- 4 Draw the inner walls.
- 5 Place the devices.
- 6 Assign badges, and view the heat maps and device coverage.

Upload a Background Image

A site map starts with a floor plan, which requires a background image that you upload. Additionally, you can delete images from ExtremeCloud.



Note

There is a limit of 200 floors per site.

The floor plan image helps you visualize the relative positioning of devices and validating whether a device can be installed in a selected location.

The following file formats are supported:

- PNG
- JPEG
- SVG (not compatible with Internet Explorer and Firefox browsers)

To upload a floor plan image:

- 1 To access the floor plan feature, select **Configure > Sites > Add > Floor Plans**. Alternatively, you can select a site from the list to edit and select **Configure Site > Floor Plans > Manage Floor Plans**.
- 2 In the **Manage Floor Plans** dialog, select **+** to add a new floor plan.



Note

You can also edit the floor plans in this list by selecting a floor plan from the drop-down menu.

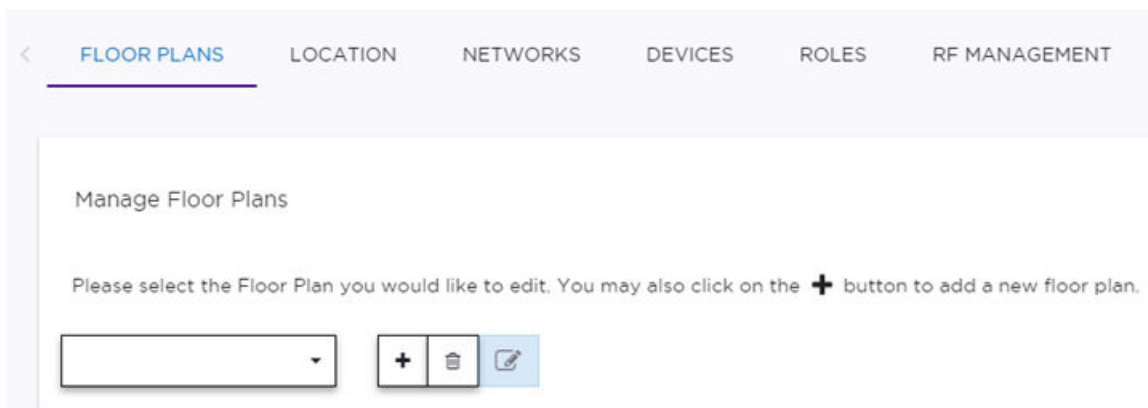


Figure 44: Manage Floor Plans

The **Add New Floor** dialog opens.

- 3 Enter a unique name for the new floor plan, and select **OK**.

Add new floor

New floor name

Floor name must be unique and not empty

CANCEL

OK

Figure 45:

- 4 In the **Draw Tools** menu that opens on the right, under **Background Image**, select **Upload**.
- 5 In your local file explorer, navigate to the location of your file. Select **Open**.

The floor plan image opens in the user interface.

Next, [set the environment and scale](#).

Specify the Environment and Scale

After you upload a floor plan, specify the environment and scale so that the tool calculates coverage accurately.

- 1 Select a site from the **Sites** list.
The site's **Dashboard** page opens.
- 2 Select **Configure Site**. On the **Floor Plans** tab, select a floor plan to edit from the drop-down list.
- 3 In the **Draw Tools** menu, select the **Environment** drop-down list and specify the type of environment for your site (Open Space, Office Cubicles, Dry Walls, Office Hard Walls, Custom). The **Custom** option lets you draw the inner walls for more coverage accuracy. For more information, see [Draw the Inner Walls](#) on page 80.

- 4 In the **Scale** section, select either **Measure** or **Doorway**.

**Note**

A door width equals approximately one meter.

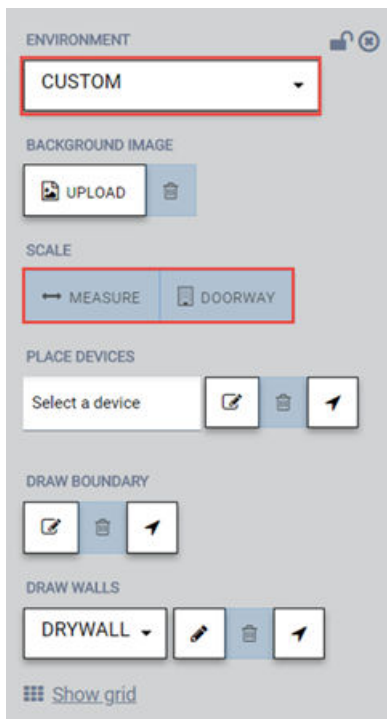


Figure 46: Environment and Scale

- 5 To anchor the beginning of the line, select a point on the map, such as one side of a doorway. As you move your cursor, a green drawing line displays.

- To anchor the end of the line, select another point on the map, such as the other side of the doorway.

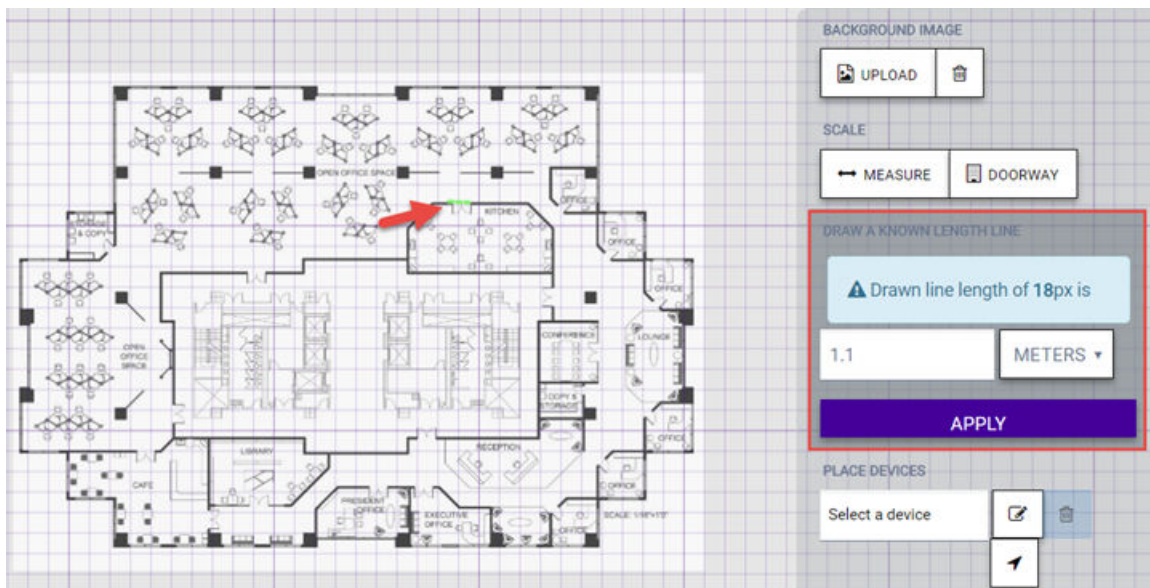


Figure 47: Completed Doorway Scale Line

- To specify the scale, select the number of feet or meters that the drawn line represents. Select **Apply**.

Next, [draw the boundary walls](#).

Draw the Boundary Walls

You must 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 the boundary walls:

- To access the floor plan feature, select **Configure > Sites > Add > Floor Plans**. Alternatively, you can select a site from the list to edit and select **Configure Site > Floor Plans > Manage Floor Plans**.
- Choose the floor map you want to edit. From the **Draw Tools** menu, under **Draw Boundary**, select . The pen tool is enabled.
- To anchor the beginning of the boundary line, select a corner of the outside boundary.
- Select 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 select and edit the boundary by selecting and dragging sections of it. Alternatively, select to remove the entire boundary and start over.

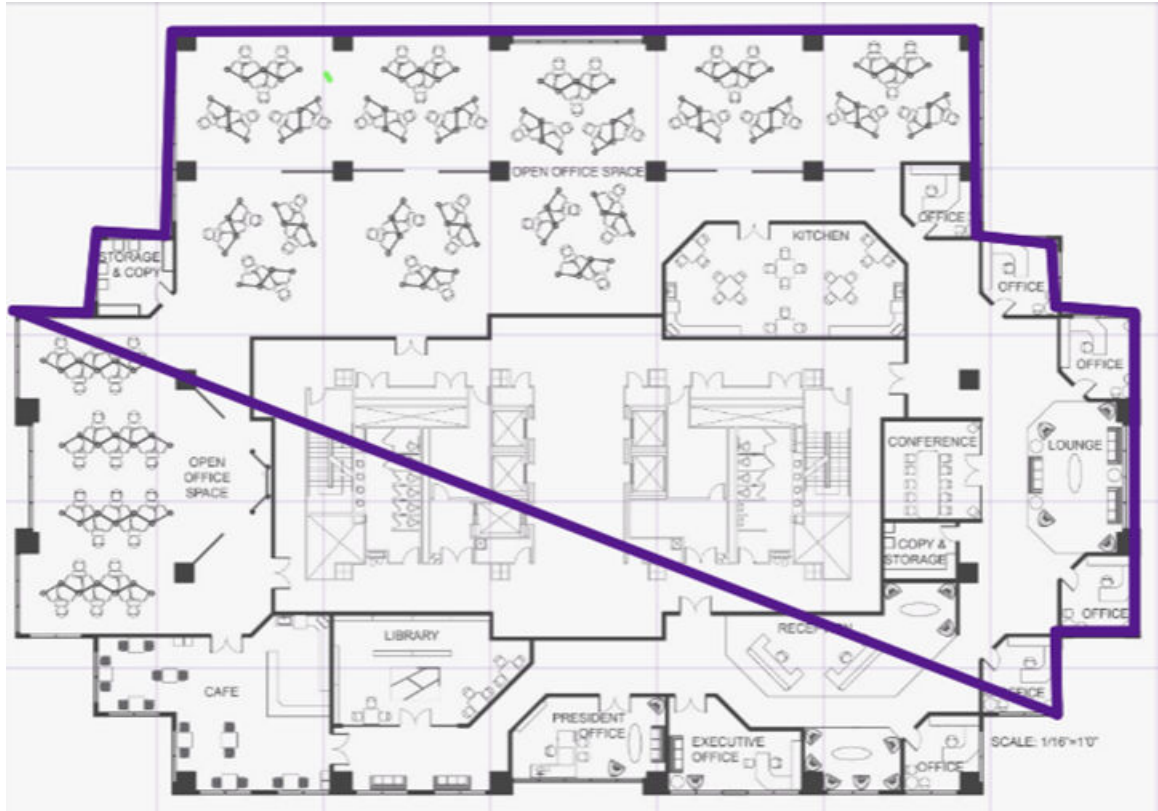


Figure 48: Drawing Boundary Walls

- When you reach the last corner (which is also your starting point), double-click the last corner to disable the pen tool.

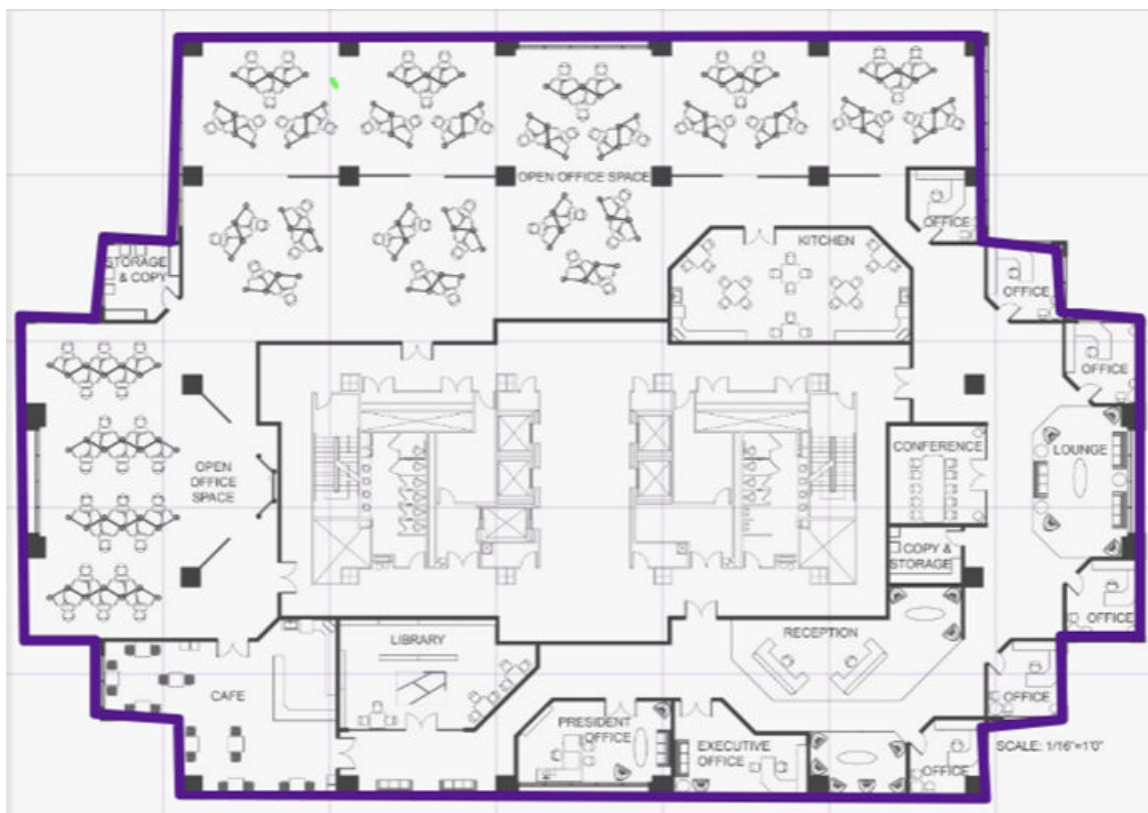


Figure 49: Completed Boundary Walls

Next, **draw the inner walls** if you selected the **Custom** environment option. Otherwise, **place your devices**.

Draw the Inner Walls

Wall materials affect the propagation and estimation models. Accurate representation of 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 drywall or cubicle walls. Office drywall has minimal impact on the floor plan propagation.



To draw inner walls for a custom environment:

- From the **Draw Walls** option, select a wall materials type from the drop-down list.
The pen tool is enabled.

- 2 To anchor the line drawing, select a corner of the inner wall.
- 3 Select each corner of the inner wall to anchor the line, and progress to the next corner.
- 4 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

You can right-click on wall to change its type or to delete it. You can also select  to edit a wall or select  to clear the inner walls and start over.

- 5 Repeat steps 2 - 4 for each area that you want to customize.

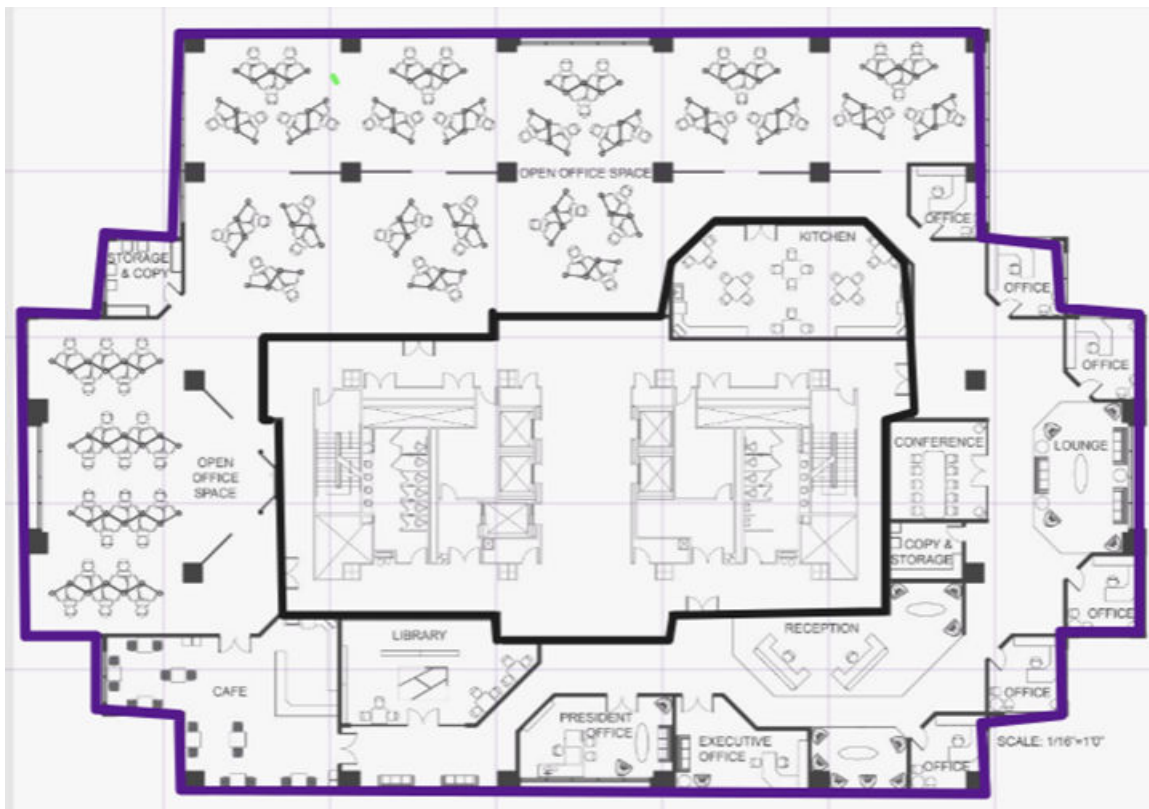


Figure 50: Concrete Inner Walls

Next, [place devices](#).

Place Devices on the Floor Plan

Manually place and configure your access points (APs) and switches.

To place the devices:

- 1 To access the floor plan feature, select **Configure > Sites > Add > Floor Plans**. Alternatively, you can select a site from the list to edit and select **Configure Site > Floor Plans > Manage Floor Plans**.

- 2 From the **Drawing Tools** menu, in the **Place Devices** section, select a device from the drop-down list, or enter the serial number in the text box to filter the list. Select the serial number in the list and then select anywhere on the floor plan to drop the device. Devices must be placed one at a time. Repeat this step as needed until all of your devices are placed.

Note




To change the placement of a device, select  and then place your cursor on the device and move it on the floor plan. To delete a device from the floor plan, right-click on the device icon and select **Delete**.

Figure 51:

- 3 (Optional) To configure the orientation of an AP, right-click on the AP in the floor plan and select **Set AP Orientation**.

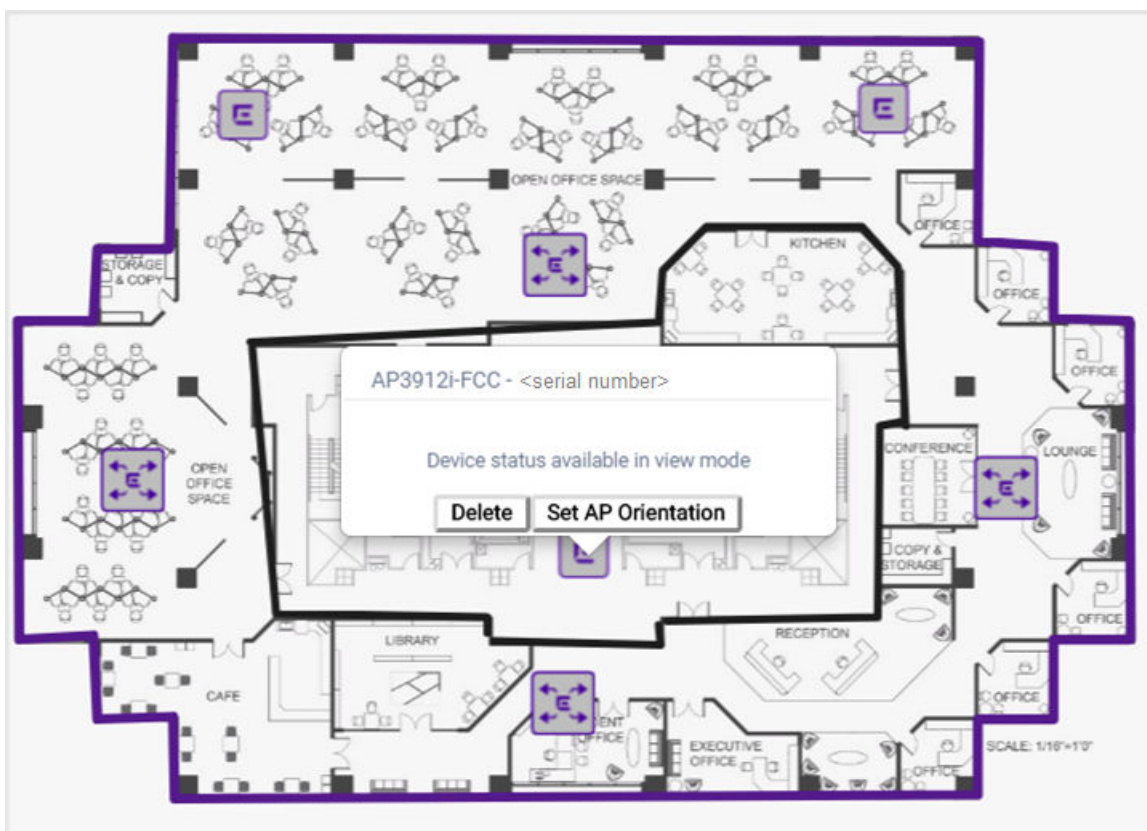


Figure 52: AP Options

- In the dialog that opens, select the mounting position, which can be either **Ceiling** or **Wall**. Select **Save**.



Figure 53: Configuring the AP Orientation

If you select **Wall**, a dialog opens that lets you specify the direction that the AP is facing.

- To specify the direction of an AP, select the directional arrow that the AP is facing. The selected arrow is marked with a Wi-Fi icon. Select **Save**.

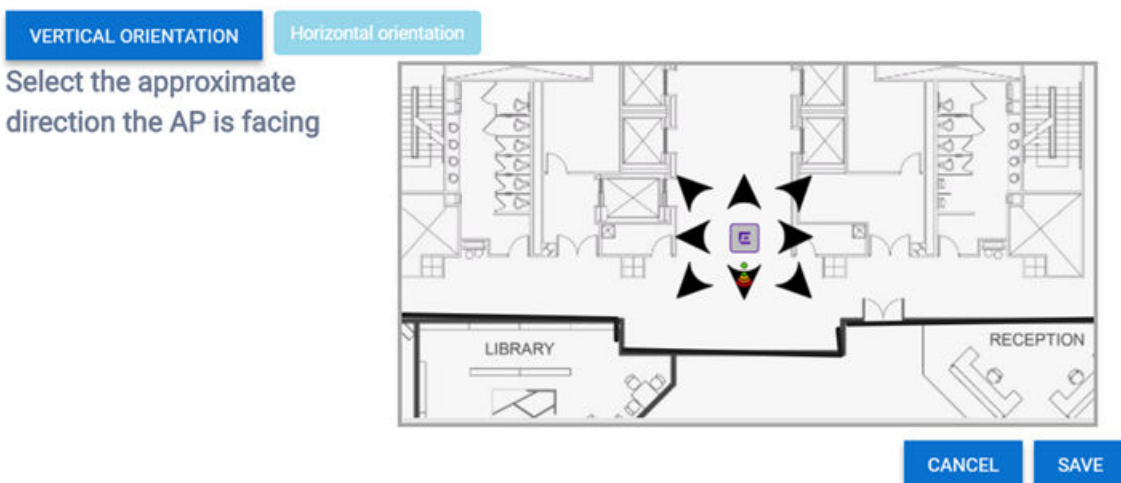


Figure 54: AP Direction Configured to the South

- To save the entire floor plan, select **Save** in the upper right corner of the **Manage Floor Plans** page. Next, [assign badges and view the device coverage](#).

Enable Badges and View Device Coverage

After you have your devices (APs and switches) placed on the floor plan, you can enable badges on APs, and view the heat maps and coverage using the map options and filters. For example, the RSS heat map tells you the coverage based on signal strength. The coverage percentage tells you what percent of the area is covered.

Right-click on an AP to see the **Context** menu, which displays links to the AP's **Dashboard** page, and the report about clients associated to the AP.

To manage badges, heat maps, and coverage:

- 1 Select a site from the list, and then select **Floor Plans**.

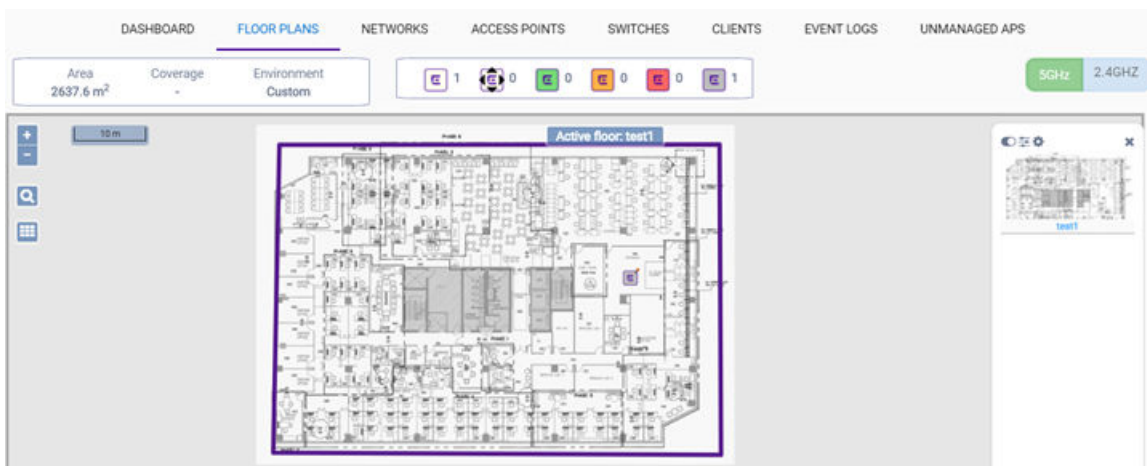


Figure 55: Floor Plan Management User Interface

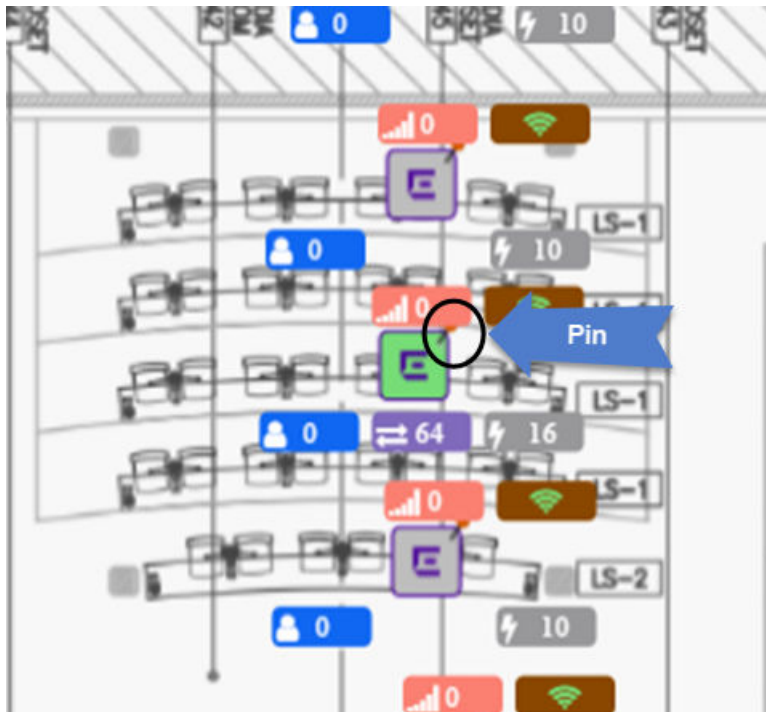


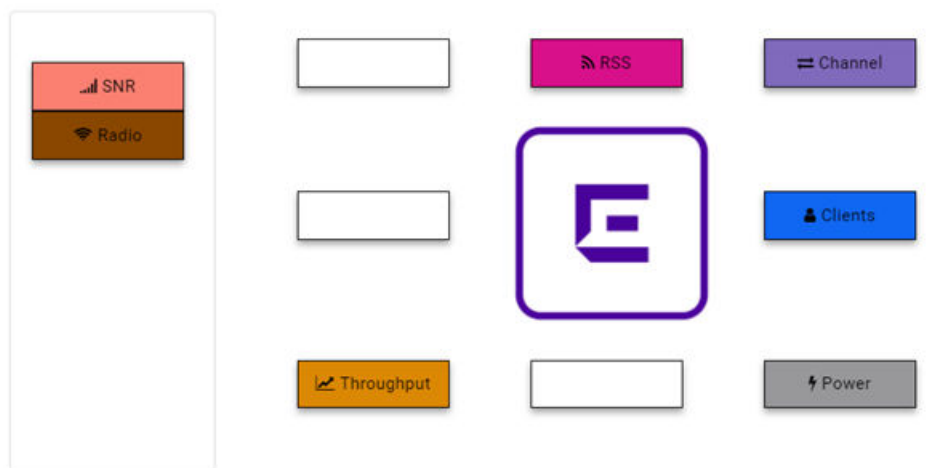
Figure 56: Active and Inactive APs Assigned to a Floor Plan

The floor plan shows all assigned devices. The APs that have a pin in the upper right corner will be included in the map simulations. The radio badge tells you whether or not the radio is on (green) or off (red). The AP icons display in different colors to show their state:

Table 12:

Color	AP State
Green	In Service
Orange	In Service/Trouble
Red	Critical
Gray	Unknown

- (Optional) Badges provide real-time statistics for APs. select the settings (cog) icon and then click **Select Badges**. In the **Badge Configuration** dialog, drag and drop the badges to the AP to include them in the display, or drag them to the left panel to exclude them from the display. Select **Save**.



To configure please drag and drop badges from the left over the placeholders on the right.
To release double-click or drag and drop badges from the placeholders into the left panel.

CANCEL

SAVE

Figure 57: Badge Configuration Dialog

The Badge Configuration dialog closes. The badges display around the APs and are visible when you zoom in on the map. To hide the badges, select **Hide Badges** from the menu on the right side of the page.

- Select the **Maps** control. By default, all of the devices on the floor plan are included in the simulation.

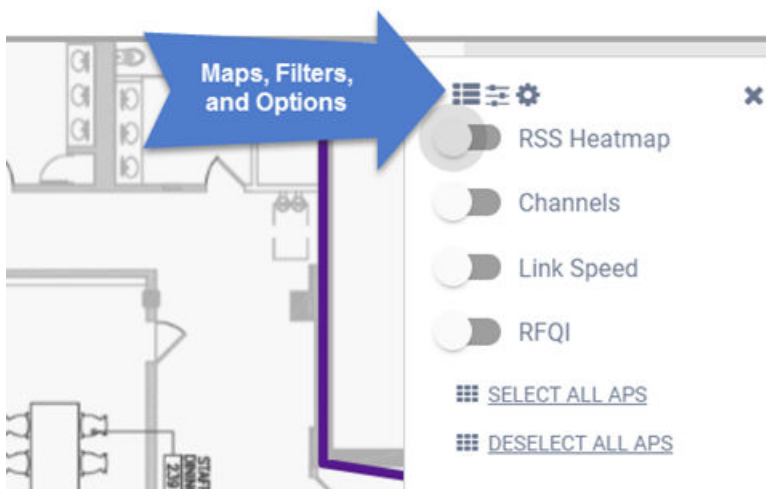


Figure 58: Controls for Maps, Filters, and Options

- (Optional) Right-click in an AP to access the **Details** and **Clients** options, which let you drill-down to the corresponding information associated with this device.

5 Select a map view.

- RSS Heat Map** Shows the device coverage. Toggle between 5 Ghz and 2.4 Ghz and visualize the differences in the heat map. Colors indicate signal strength. Red indicates the strongest signal. Blue indicates the weakest signal. Heat maps are automatically recalculated when a change is detected in the device configuration.
- Channels** Shows a visualization of the channel plan. Colors indicate primary channels for each AP, illustrating competing neighboring channels. Channels are useful for 2.4 GHz APs where neighboring APs on the same channel should be avoided.
- Link Speed** Displays the expected internal WLAN connection speed between the wireless clients and the APs.
- RFQI** Identifies access points with poor RF quality. The labels are color coded to indicate overall RF quality of the AP, based on the signal strength of the clients connect to them.

The selected map renders a visualization on the floor plan.

6 (Optional) To show only APs whose runtime (badge) data is within a certain range, use the **Filters** option. The following filters are available:

Figure 59: Filter Options

- Min RSS** Shows the APs that are within the range of the minimum received signal strength (RSS) indicated by the slider control.
- RFQI** Shows the APs that are within the range of the radio frequency (RF) quality indicated by the slider control.
- Power** Shows the APs that are within the range of the radio transmit power indicated by the slider control.
- Channel** Shows the APs that are within the range of the channels indicated by the slider control.
- Map Opacity** Makes the view of the background image more or less opaque as indicated by the slider control.

- | | |
|-------------------|--|
| SNR | Shows APs that are in the range of the signal-to-noise ratio (SNR) indicated by the slider control. SNR is the ratio between the strength of the signal and the background noise on the line. This value is measure in decibels (dB). |
| Throughput | Shows the APs that are within the range of the throughput indicated by the slider control. |
| Clients | Shows the APs that are within the range of clients indicated by the slider control. The range can be from 0 - 200 clients. |
| RSS | Shows the APs that are within the range of the received signal strength, measured in dBm, indicated by the slider control. No less than three APs should be detecting and reporting the RSS of any client station. Only RSS reading stronger than -75 dBm are used by the Location Engine. |
- 7 After you adjust the filters and maps, and optionally toggle between radio frequencies, you can readjust your coverage by **moving the devices around** and then viewing the changes in the coverage.

Configure a Site Location

The **Sites** main page displays site location on a physical map. The physical map makes it convenient to view multiple sites. Select a site location from the map to access the individual site dashboard and site management tools.

To add a site location to the physical map:

- 1 Select **Configure > Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName > Configure Site**, or select **Add** to add a new site.
- 3 Select the **Location** tab.

- 4 Enter the Site Manager contact information.

Figure 60: Location Configuration

- Site Manager Name
 - Site Manager Email
 - Site Manager Contact
 - Region
 - City
 - Campus
- 5 For the **Map Coordinates**, either select a location on the map to automatically populate the coordinates, or manually enter the longitude and latitude, separated by a comma delimiter. **Example:** -78.638179, 35.779590.
 - 6 Select **Save**.

Assign Networks to a Site

A default site has a default network (wireless SSID) assigned to it. A network service consists of a policy that defines network traffic, authentication type, and role. We recommend configuring the default settings for the default network service or creating a new network service.

If you create a new network (wireless SSID), you must add the network to a site to activate the new network services to the wireless devices at that site.

Multiple network services can be applied to a site.

To assign networks to a site:

- 1 Select **Configure > Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName > Configure Site**, or select **Add** to add a new site.

- 3 On the **Networks** tab, select a network and assign the network to a specific radio.

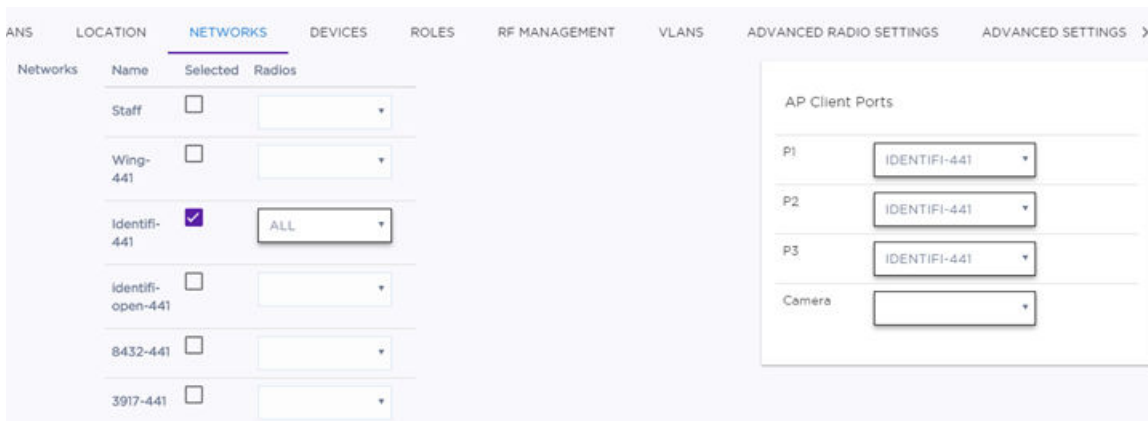


Figure 61: Network Configuration for a Site

- 4 Some AP models have wired client ports, which are Ethernet ports to which host computers can be connected. The **AP Client Ports** pane displays any APs that have wired client ports. Assign one network to each wired client port. A wired client port must have exactly one network assigned to it in order to operate.



Note

The number of ports that display depends on the AP model.

AP3916ic also has a camera port that can be assigned to a network with filters. The camera port supports all policy rules and actions, except that it can be assigned only to an untagged VLAN. An open WLAN can be assigned to the camera port. By default, the camera port is assigned to a network with a Deny All policy. This means that you will not be able to stream traffic to or from the camera until this Deny All policy is replaced.

- 5 Select **Save**.

Configure Device Adoption Rules

If you have multiple sites, you can use adoption rules to automatically assign access points (APs) and switches to a site when devices are registered for the first time. The adoption rules determine which site the devices are assigned to based on the attributes that the device communicates to the cloud. Each site can have its own adoption rules. Without adoption rules, each device must be manually assigned to a site.




Note

Configure the adoption rules before registering the devices.

To configure adoption rules:

- 1 From the left menu, select **Configure > Adoption**.

- 2 Select **Add**. Alternatively, select an existing rule and select  .
The **New Rule** dialog opens.

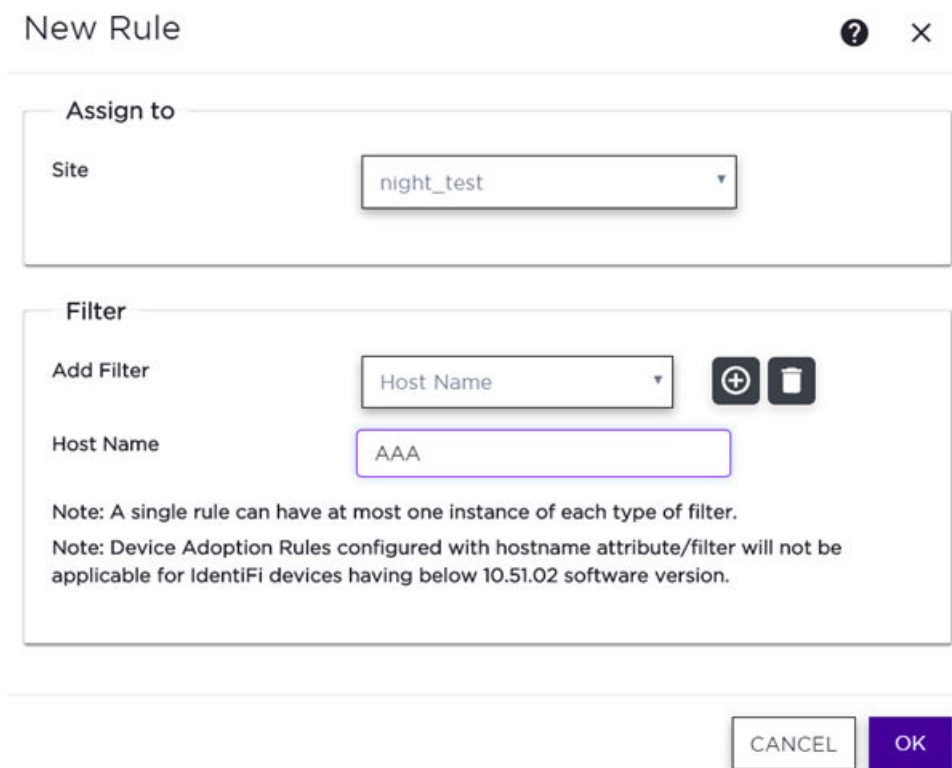


Figure 62:



- 3 For **Site**, select the site name from the drop-down list.
4 For **Add Filter**, the fields that display depend on which filters you choose. Configure one or more filters as needed.

Private IP Address / CIDR	Enter a single IP address for each rule, and a CIDR value between 1 - 30.
Host Name	Enter the matching criteria as a sub-string or as an exact match. The search is case-sensitive. The maximum length is 255 characters.
Model	Enter a matching criteria as a sub-string or as an exact match. For example, if the filter criteria is the substring FCC , all APs with FCC in the model number will match. The search is case-sensitive.
Serial Number	Enter the matching criteria as an exact string. Enter a single serial number for each rule.

- 5 In the Adoption Rules list, use the up and down arrows to change the order of the adoption rules. Rules are evaluated and applied based on the order in which they display, from the top down. If a device does not match the criteria of first adoption rule, the next rule is evaluated. The devices are automatically assigned to the site based on the first matching adoption rule definition. If no rule matches, the device is either orphaned or put into the default site that matches the device's regulatory domain (such as FCC, WR, and so on).



Note

Use the pencil icon () to edit the rule, or the trash icon () to delete the rule.

Site	Private IP Address	CIDR	Host	Model	Serial Number
Default	Any	Any	Any	AP3965I-FCC	Any
night_test_wing	Any	Any	Any	AP510-FCC	Any
night_test	Any	Any	AAA	Any	Any

Figure 63: Adoption Rules List

- 6 Select **Save**.

Assign Devices to a Site

A site consists of the access points and switches that are managed by the site's configuration. (Additional configuration can be made for individual devices, such as port management and channel plans.)

To assign devices to a site:

- 1 Select **Configure > Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName > Configure Site**, or select **Add** to add a new site.
- 3 On the **Devices** tab, assign access points and switches from the lists of available devices.

APs		Switches	
Name	Selected	Name	Selected
1703Y-1004000000	<input type="checkbox"/>		
1714Y-1039300000	<input type="checkbox"/>		
1730Y-1019000000	<input type="checkbox"/>		
AP-3915-Ext	<input checked="" type="checkbox"/>		
1803Y-1989900000	<input checked="" type="checkbox"/>		

Figure 64: Devices Tab

- 4 Select **Save**.

Assign Roles to a Site

A *role* is a set of network access services, such as authentication type, that can be applied at various points in a policy-enabled network. Roles are usually named for a type of user such as Student, Staff, or Guest. (Roles can optionally contain rules that provide different treatments for different packet types to which a single role is applied.)

When you create a site, a default role is applied. If you are using a RADIUS server, you must configure the default role for the site. Otherwise, this procedure is optional.

To assign and optionally configure roles for a site:

- 1 Select **Configure** > **Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName** > **Configure Site**, or select **Add** to add a new site.
- 3 On the **Roles** tab, assign a role.

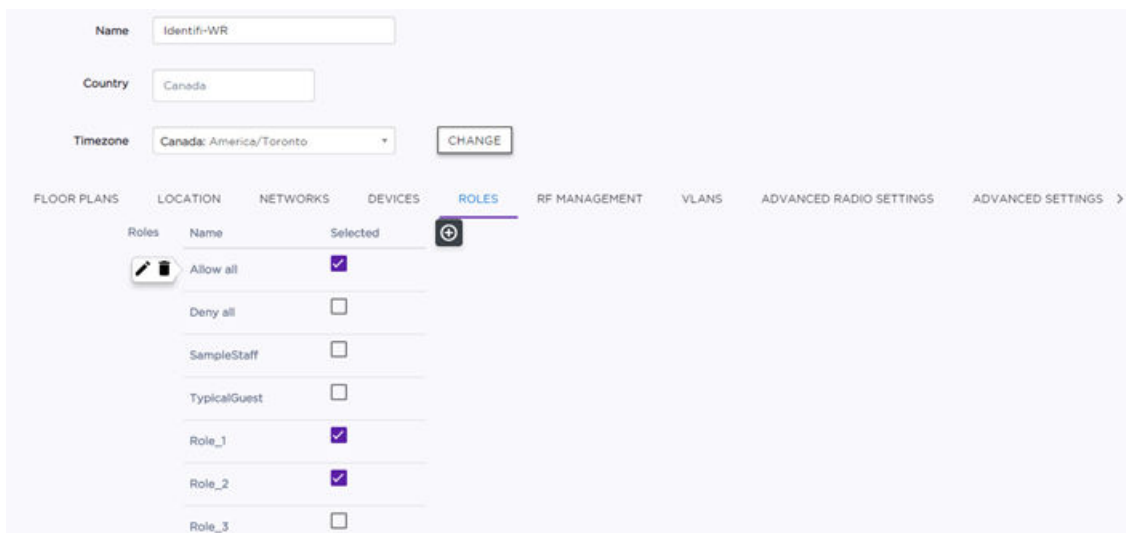


Figure 65: Roles Tab

- 4 (Optional) You can also **add a role**, or hover over an existing role and select  to edit it.



Note

To delete a role, select  (Trash icon).

- 5 Select **Save**.

Configure RF for a Site

RF management for access points (APs) is configured at the site level. A site is automatically created with default RF settings to simplify the complex task of RF management. Additional configuration is optional.



Note

For more information about the RF management options, see [RF Management Options](#).

To configure RF:

- 1 Select **Configure** > **Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName** > **Configure Site**, or select **Add** to add a new site.
- 3 Select the **RF Management** tab.

4 (Optional - ExtremeWireless WiNG APs Only) Enable SMART RF by editing the following fields.

Smart RF Sensitivity	Specify the Smart RF sensitivity, which in turn affects the Interference recovery value as follows: <ul style="list-style-type: none"> Low When specifying low, the Interference Recovery value is set to Aggressive. Smart RF will only enable compensation from neighboring radios if the signal to noise ratio for a wireless client, as seen by the access point, exceeds the value specified for Interference Recovery. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below this threshold. Medium When specifying medium, Interference Recovery value is set as a value between Conservative and Aggressive. This is the default value. High When specifying high, Interference Recovery value is set to Conservative.
Interference Recovery	Enables compensation from neighboring radios when radio interference is detected. When interference is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client (as seen by the access point radio). If a client's signal-to-noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. Default: Enabled
Coverage Hole Recovery	Enables coverage compensation from neighboring radios when a radio coverage hole is detected within the Smart-RF supported radio coverage area. When coverage hole is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client as seen by the access point radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. Default: Enabled
Neighbor Recovery	Enables automatic recovery by instructing neighboring access points to increase their transmit power to compensate for the coverage loss. Default: Enabled
Off-Channel Scan	Forces Smart RF to scan all channels once per day during off-peak hours. If you are enabling the WIDS option (on the Advanced Settings page), then enabling Off-Channel Scan when disabling Smart RF causes the AP to scan other channels for threats. If WIDS is enabled and Smart RF is enabled, then the AP detection will piggyback on the off-channel scan under the control of Smart RF.

- 5 (Optional - For ExtremeWireless WiNG Only) Configure the radio settings. The settings apply to all AP radios at the site only if you configure each device to use the site-level RF settings for the 5GHz band, 2.4 GHz band, or both bands.

The screenshot displays the configuration interface for ExtremeWireless WiNG APs. At the top, there are two sliders for SNR thresholds: '2.4 GHz SNR Threshold' and '5 GHz SNR Threshold', both set to 20. Below these are three toggle switches: 'Coverage Hole Recovery' (on), 'Neighbor Recovery' (on), and 'Off Channel Scan' (off). A note under 'Off Channel Scan' states 'Scan for all channels and devices once per day.' The main configuration area is split into two columns: 'Radio 5 GHz' and 'Radio 2.4 GHz'. Each column has a 'VIEW' button at the bottom. The settings for both bands are as follows:

Setting	Radio 5 GHz	Radio 2.4 GHz
Client Aware Scanning	0 Disabled	0 Disabled
Voice Aware Scanning	<input checked="" type="checkbox"/> (dynamic)	<input checked="" type="checkbox"/> (dynamic)
Channel Width	AUTO	AUTO
Min Tx Power [dBm]	10	10
Max Tx Power [dBm]	16	16
Channel Plan	ALL CHANNELS BY COUNTRY	AUTO

Figure 66: Radio Settings for ExtremeWireless WiNG APs

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.

Voice Aware Scanning Specify how voice aware recognition is configured for Smart RF. **Dynamic** disables smart monitoring when buffered data exists at the radio for a voice client. **Disable** specifies that the Voice Aware Scanning option will not be used at all. **Default:** Dynamic (for both the 5 GHz and 2.4 GHz bands)

Channel Width Channel width helps to improve the effective throughput of the wireless LAN. Pick the channel mode that best suits the density of the deployment to avoid co-channel interference.

20 MHz Recommended for larger density deployments of greater than 10 APs.

40 MHz Recommended for deployments of 5 - 10 APs.

80 MHz Channel bonding is enabled. Recommended for deployments of less than five APs.



Note

The 160 MHz channel width is not supported for AP505 and AP510.

Auto Automatically switches between 20 MHz and 40 MHz, depending on how busy the extension channel is.

- Min Tx Power (dBm)** Specify the minimum power level for the radio. Use the lowest supported value in order to not limit the potential transmission (Tx) power level range that can be used. The Min Tx Power setting cannot be set higher than the Max Tx Power setting.
- Max Tx Power** Specify the maximum transmission power. The values are in dBm and vary by AP. The Max Tx Power should be set at a higher power level than the Min Tx Power.
- 6 **(Optional - For ExtremeWireless Only)** Configure the settings for the radios. The settings apply to all AP radios at the site only if you configure each device to use the site-level Smart RF settings for the 5GHz band, 2.4 GHz band, or both bands.
- DCS Noise Threshold (dBm)** Define the noise interference limit, measured in dBm. If the noise interface exceeds this threshold, Automatic Channel Scan (ACS) scans for a new operating channel for the AP.
- DCS Channel Occupancy Threshold** Define the channel utilization level, measured as a percentage. If the threshold is exceeded, ACS scans for a new operating channel for the AP.
- DCS Update Period (Minutes)** Define 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 ACS.
- Interference Wait Time (Seconds)** Specify the length of the delay (in seconds) before logging an alarm. **Default:** 10 seconds
- Min Tx Power (dBm)** Specify the minimum power level for the radio. Use the lowest supported value in order to not limit the potential transmission (Tx) power level range that can be used. The Min Tx Power setting cannot be set higher than the Max Tx Power setting.
- Max Tx Power** Specify the maximum transmission power. The values are in dBm and vary by AP. The Max Tx Power should be set at a higher power level than the Min Tx Power.
- 7 **(Optional - For All AP Types)** Select **View** to configure the Channel Plan options. The options that display depend on the radio's band (2.4 GHz or 5 GHz).
- Channel Plan** If Smart RF is enabled on either radio, you can define a channel plan for the AP that limits which channels are available for use during an Smart RF scan. For example, you may want to avoid using specific channels because of low power, regulatory requirements, or radar interference.
- All Channels** (5.0 GHz radios only) Scans all channels for an operating channel. Returns Dynamic Frequency Selection (DFS) channels and non-DFS channels, if available.
- Custom Channels** When this option is selected, the **Configure** button displays for configuring individual channels from which the Smart RF selects an operating channel.
- All Channels by Country (Non-DFS)** (5.0 GHz radios only) Scans all non-DFS channels by country for an operating channel. This selection is always available, but if there are no DFS channels available, the list is the same as the All Channels list.
- All Channel by Country** (5.0 GHz radios only) Scans all channels by country for an operating channel. Returns DFS and non-DFS channels, if available.
- 3 Channel Plan** (2.4 GHz radios only) Scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in most other parts of the world.
- 4 Channel Plan** (2.4 GHz radios only) Scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in most other parts of the world. Applicable to 2.4 GHz radios only.
- Auto** Scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in most other parts of the world.
- 8 Select **Save**.

Configure Advanced Radio Settings

Advanced radio settings for access points (APs) can be configured at the site level and will apply to all APs at the selected site.

To configure the advanced radio settings:

- 1 Select **Configure** > **Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName** > **Configure Site**, or select **Add** to add a new site.
- 3 (Optional) On the **Advanced Radio Settings** tab, configure advanced radio settings.



Note

Some settings only apply to and some only apply to WiNG.

	Radio 2.4 Ghz	Radio 5 Ghz
Min Basic Rate for Radios (Mbps)	6 ▾	6 ▾
Aggregate MPDU +	ENABLED ▾	ENABLED ▾
STBC +	DISABLED ▾	DISABLED ▾
Tx Beam Forming +	DISABLED ▾	MU_MIMO ▾
Trigger Site-Wide Channel Selection +	ENABLE	ENABLE

Note : (+) denotes IDENTIFI only attributes and (-) denotes WiNG only attributes

Figure 67: Advanced Radio Settings

Radio Share Mode	Radio operates as a sensor and a traffic forwarder. Valid values are:
Off	Disables the Radio Share capability.
Inline	The AP reports to the ADSP server only the multicast / broadcast traffic, such as beacons and probe requests. Inline mode has minimal impact on the AP performance, because the AP only reports (to the ADSP server) the traffic that it processes.
Promiscuous	The AP receives all of the packets It sees on its operating channel and forwards them to the ADSP server. Promiscuous mode loads the AP resources, because AP has to process all of the traffic in the channel. In high-density, wireless

deployments, use dedicated sensors instead of Radio Share in Promiscuous mode.



Note

Set the AP to Promiscuous mode when the AP is required to perform termination.

Min Basic Rate for Radios Select the minimum data rate that must be supported by all stations in a BSS: 6, 12, or 24 Mbps. Min Basic Rate is used for connecting the clients to the BSS. Data rates used for traffic are higher or equal to the Min Basic Rate, and depend on client capabilities and environment conditions. Only mixed mode (ANC or GN) is supported. Strict mode (n-strict and ac-strict) is not supported, therefore, HT minimum basic rates are not supported.

Aggregate MPDU Enable Aggregate MPDU for significant improvement in throughput.

STBC STBC is a simple open loop transmit diversity scheme. When enabled, STBC configuration is 2x1 (two spatial streams combine into one spatial stream). TXBF overrides STBC if both options are enabled for single stream rates.

Tx Beam Forming Enable Transmit Beam Forming to get better signal-to-noise ratio on the receiver side. This option is not applicable to all AP models.

Trigger Site-Wide Channel Selection To enable [Automatic Channel Selection \(ACS\)](#) on an AP radio for a site, select either **Radio 1** or **Radio 2**. The command is sent to one of the APs in the site, and the AP negotiates channel selection with other APs in the group. Automatic Channel Selection is per radio. (The operating channels that were chosen can be viewed after you save your changes by selecting **Sites** and viewing the **Networks** tab for a specific site.)

- 4 Select **Save**.

Assign VLANs to a Site

VLANs define how the user traffic is presented through the network interface. VLAN IDs can be applied at the site level. This procedure is optional.



Note

[VLANs are configured as part of a policy](#). For more information about VLANs, see [Tagged and Untagged VLANs](#) and [VLAN Groups](#).

To assign VLANs to a site:

- 1 Select **Configure** > **Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName** > **Configure Site**, or select **Add** to add a new site.

- 3 On the **VLANS** tab, select one or more VLANs in the list.

Figure 68: VLANS Tab

- 4 (Optional) Select a VLAN name in the list to open the VLAN configuration dialog. Select **Advanced** to [configure the VLAN settings](#).

Important



Including multiple VLANs in the VLAN IDs field will cause ExtremeWireless WiNG APs to load balance traffic across all the listed VLANs. This is an advanced option and should only be enabled in special cases. APs will use the lowest numbered VLAN in the list and will not load balance across the VLANs.

- 5 Select **Save**.

Configure Advanced Settings for Sites

Advanced settings for sites let you enable system log (syslog), SNMP, band steering, DNS server, and automatic channel selection for a site. You can also schedule site within a 2-week period of the upgrade availability. The options that display depending on the AP models that you have deployed at your site.

- 1 Select **Configure > Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName > Configure Site**, or select **Add** to add a new site.

- 3 Edit the fields in the **Advanced Settings** dialog. The fields that display depend on whether you enable SNMP and the type of SNMP you select.

The screenshot shows the 'Advanced Settings' dialog for Sites. The 'ADVANCED SETTINGS' tab is selected and highlighted with a red box. The settings are as follows:

- Enable DPI:
- Band Steering: DISABLED
- Upgrade Schedule: CHANGE, RESET
- SNMP: DISABLED
- System Log: DISABLED
- WIDS: DISABLED
- ExtremeLocation: DISABLED
- Enforce Version: MAJOR

Figure 69: Advanced Settings for Sites

- Enable DPI** Enable or disable application recognition and control using Deep Packet Inspection (DPI) at this site. DPI is used to identify, classify, route or block packets based on the contents of the packet.
- Band Steering** Enable or disable band steering for all of the APs in the site. For example, enabling band preference lets you move an 11a-capable client to an 11a radio to relieve congestion on an 11g radio.
- Upgrade Schedule** (Optional) The ExtremeCloud Operations team sets the default upgrade schedule. You can do nothing and accept the default schedule, or you can schedule an upgrade within the 2-week default schedule. Select **Reset** to revert your edits to the default upgrade schedule. Keep in mind the following information:
- If an upgrade cycle is in progress and you change the day that the site will be upgraded, the change will be implemented as long as the new day is at least a day ahead in the calendar.
 - If an upgrade cycle is *not* in progress, the configuration will be saved and the next upgrade cycle will be based on it.
 - When *resetting*, if upgrade cycle is in progress and you try to reset the previously saved preferred time as **No preference**, the request is ignored and the schedule continues with the previously selected time. **Example:** If the upgrade cycle starts on Monday and your preferred site upgrade time is saved as **Week 1, Thursday at 5 PM**, and then you try to reset site upgrade time as **No preference**, the site upgrade will take place on **Week 1, Thursday at 5 PM**.
- 4 (Optional) Enable Simple Network Management Protocol (SNMP) for retrieving statistics and configuration information for the switches in a site. Choose either SNMPv2c or SNMPv3 and edit the fields that display.
- SNMPv2c** Configure SNMP communities and notifications. READ_LEVEL is the only available access; the SNMP profile will have read-only SNMP communication.
- SNMPv3** Configure SNMP users. These are global users that you can add to SNMP profiles.
- | | |
|------------------|---|
| Name | Specify a unique name for the user account. |
| Auth Type | Select an authentication protocol from the drop-down list. This applies only if the Security level will be set to Authentication / No Privacy or Authentication / Privacy. |

Auth Password	Specify and confirm the authentication password if the Security level will be set to Authentication / No Privacy or Authentication / Privacy.
Privacy Type	Specify either AES or DES privacy protocol if the Security level will be set to Authentication / Privacy.
Privacy Password	Specify and confirm the privacy password if the Security level will be set to Authentication / Privacy.
Access Level	Specify whether this user will have Read, Read/Write, or Super User access.
Security	Select an option from the drop down list to specify whether authentication and privacy will be required for this user.

- 5 (Optional) Configure **SNMP Notifications**. You can also import existing SNMP notifications from a server.
- 6 (Optional) Enable or disable **System Log** for the streaming of system log messages for ExtremeWireless WiNG APs or for switches that are used with ExtremeWireless APs in a site. When configuring this option for ExtremeWireless WiNG APs, you can also enable or disable **Guest Traffic Log**. **Default:** Disabled
- 7 (Optional) Configure the **WIDS** option.

WIDS (ExtremeWireless WiNG only) Scans Wireless Intrusion Detection Services (WIDS) for threats. When enabled, all detected threats are reported when they start and when they stop. If **Enable Off Channel Scan** is selected and if Smart RF is disabled for the site, the AP scans other channels for threats. However, if Smart RF is enabled for the site, then the AP detection will piggy back on the off-channel scan under the control of Smart RF. **Default:** Disabled
- 8 (Optional) Enable the **Location** field if you have an ExtremeLocation account, and specify the reporting interval.
- 9 (ExtremeWireless WiNG only) **Enforce Version** prevents mixing the firmware versions of ExtremeWireless WiNG APs assigned to a site. During AP registration, APs that are not compatible with the setting are orphaned. **Default:** Major

Major Allows site adoption of the AP only when the first two octets of the firmware versions match, such as 5.1. This means that all APs at the site must run the same major release (except in the upgrade window). This is the default setting.

None Allows site adoption of APs with any version.



Note

There is no guarantee that mixing the firmware versions will be compatible. The best practice is to use **Major**.

- 10 Select **Close**.
You return to the **Configure Site** page.
- 11 Select **Save**.

If you enabled location analytics, go to **Settings > General > ExtremeLocation > Account Number** and enter your ExtremeLocation account number.

IoT Services

Internet of Things (IoT) service is available on supported access points (APs) for the following applications:

ExtremeWireless APs (with IoT hardware)

- iBeacon
- Eddystone-url Beacon
- Thread Gateway

ExtremeWireless WiNG APs (with IoT hardware)

- iBeacon
- Eddystone-url Beacon



Note

For a list of supported APs with IoT hardware, see the **ExtremeCloud** Release Notes.

IoT services are assigned at the site level, with one IoT service per site. The IoT configuration is applied to all APs at the site that support IoT. APs that do not support IoT are ignored by the IoT configuration. The IoT services that are available depend on whether the site is an ExtremeWireless or ExtremeWireless WiNG site. Thread gateway offers the ability to configure whitelists.

No IoT statistics are collected or reported on at this time.

APs that have an external Bluetooth antenna can configure the antenna using the Professional Installation Screen.

More Information

- [Configure an IoT Service](#) on page 102

Configure an IoT Service

IoT services are assigned at the site level, with one IoT service per site. The IoT configuration is applied to all APs at the site that support IoT. APs that do not support IoT are ignored by the IoT configuration. The IoT services that are available depend on whether the site is an ExtremeWireless or ExtremeWireless WiNG site. Thread gateway offers the ability to configure whitelists.



Note

For a list of supported APs with IoT hardware, see the [ExtremeCloud Release Notes](#)

To configure an IoT service:

- 1 Select **Configure** > **Sites** from the menu.
The **Sites** list displays.
- 2 From the **Sites** list, select **siteName** > **Configure Site**, or select **Add** to add a new site.
- 3 Select the **IoT** tab.

- 4 In the **Application** field, select an IoT service from the drop-down list.

The corresponding fields display.

Application	THREAD GATEWAY
Network Name	networkname1
Channel	25
Short PAN ID	0ACB
Extended PAN ID	9F59610646BB6EF3
Master Key	DCDA919EE30EC38A2AE03B75C3487342
Common Credentials	THREADNETWORK
IoT Radio Service	SERVICE_1
	WHITELIST

Figure 70: Example of Thread Gateway Configuration

- 5 If **iBeacon** was selected, edit the fields as follows:

Advertising Interval Specify the how often, in milliseconds, your beacon will transmit its advertising packet. **Values:** Min (100ms) and Max (10240ms). **Default:** Min (100ms)

UUID An identifier used to differentiate a large group of related beacons. Specify the UUID for which you want to filter data. **ExtremeCloud** forwards the data that matches the specified UUID and filters out all other UUID data. If the UUID configured value is all zeros, no filtering occurs.

Major Specify a subset of beacons within the larger UUID set. This value can represent a venue specific attribute, such as a specific store or a wing in a building. **Values:** 0 to 65635

Minor Specify an individual beacon whose location you want to more precisely pinpoint. 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. **Values:** 0 to 65635

- 6 If **Eddystone-URL** was selected, edit the fields as follows:

URL Specify the URL that is included with the Eddystone-url beacon. **Limit:** 17 characters. The 17 characters does not include the protocol, but it does include the domain name. The URL is compressed, effectively allowing more than a 17 character input. See <https://github.com/google/eddytone/tree/master/eddytone-url> for the Eddystone-url compression rules to more accurately judge the length of your URL. If necessary, search for third-party URL shortening services available on the Internet.

Advertising Interval Specify the how often, in milliseconds, your beacon will transmit its advertising packet. **Values:** Min (100ms) and Max (10240ms). **Default:** Min (100ms)

- 7 If **Thread Gateway** was selected, edit the fields as follows:

Network Name Specify a network service name. The networks service provides the policies that will be used for the thread network.

- | | |
|--------------------------|--|
| Channel | Specify the IEEE Standard: 802.15.4 AP channel number. |
| Short PAN ID | Specify the Personal Area Network (PAN) identifier as a 16-bit short address, which uniquely identifies the AP thread network. The PAN ID is part of the MAC-layer and is used in RF data transmissions between devices in a thread network. The default value is derived from the AP serial number. |
| Extended PAN ID | Specify the unique 64-bit MAC-layer address, which provides more specific network identification than the short PAN ID. PAN IDs are used in RF data transmissions between devices in a thread network. The default value is derived from the AP serial number. |
| Master Key | Specify the network master key used to encrypt communication between nodes in a thread network. |
| IoT Radio Service | Select the network service that the AP radios will use for IoT management. |
- 8 (Thread Gateway only) To configure a whitelist, select **Whitelist**. This step is optional. The **Whitelist** dialog opens.
 - 9 (Thread Gateway only) Edit the fields in the **Whitelist** dialog:

Extended Unique Identifier (EUI)	Specify the unique ID of the IPv6 interface that will be allowed access to the thread network. Limit: 16 hex characters
Password	Specify the password for the EUI. Limit: 32 characters
 - 10 Select **Save**.

For APs with an external IoT antenna, configure the antenna settings in the **Professional Install** dialog for an **ExtremeWireless** AP or an **ExtremeWireless WING** AP. The antenna is configured at the device level, not at the site level.


Configure AirDefense Profiles

A cloud-managed access point (AP) can integrate with the Extreme AirDefense® Service Platform, which allows the AP to function as an AirDefense sensor, or to act as a sensor and retain the ability to forward traffic.

In dedicated sensor mode, the AP operates independently from **ExtremeCloud** while **ExtremeCloud** continues to see the AP and display the AP role as a dedicated AirDefense sensor. In its role as a dedicated sensor, the AP does not report statistics to the **ExtremeCloud**.

If a site is deleted, the associated profile is deleted.

To configure an AirDefense profile:



- 1 Do one of the following actions from the left menu:
 - Select **Configure > Sites**. Select or add a site. Scroll right to the **Air Defense** tab.
 - Select **Configure > Air Defense**.
- 2 To add a new profile, select **Add** or . Alternatively, select an existing profile from the list to edit or copy.



Note

A profile that is associated with a site cannot be used by other sites. However, you can clone an existing profile to create a new profile if the AirDefense configuration is the same for multiple sites.

3 Edit the fields.

Name	Enter the name of the AirDefense profile.
Add Server IP Address	Enter the IP address of the AirDefense servers as an FQDN or IPv4 string. To add the IP address to the Server IP Addresses list, select  . Limit: 255 characters maximum
Port	Use the default port or, for WiNG, you can configure a different port for the profile. Each IP address and port pair represents one AirDefense server, with a maximum of three IP or port pairs. Default Port: 443
Servers	Displays the list of server IP addresses that are assigned to the profile. Select  to remove an IP address from the list.


4 Select **Save**.

The profile is assigned to all APs at the site. If you added the profile from the **Sites > ADSP** tab, the profile is assigned to the selected site. If you added or edited the profile from the **Configure > ADSP Profiles** page, the profile is mapped to the site you selected from the Sites list on that page.

Remove AirDefense Integration

Extreme AirDefense integration can be removed from a site.

To remove the integration:

- 1 From the left menu, select **Configure Site**.
- 2 Select the right arrow and scroll right to the **Air Defense** tab.
- 3 Select , then select the blank line from the drop-down list.
- 4 Select **Save**.

Clone a Site

To save effort, you can clone a site that is similar to an existing site, and then make changes to the clone.



Note
Everything except the floor plan will be cloned.

To clone a site:

- 1 Select **Configure > Sites** from the menu.
The **Sites** list displays.
- 2 Select a site from the list. Select **Configure Site > Clone**.
The **Clone** dialog opens.
- 3 Enter a unique name for the clone.
- 4 Select **OK**.



Note
To cancel the action, select **Cancel**.

The cloned site is created. Edit the cloned site as needed and configure a new floor plan.

Delete a Site

To delete a site:

- 1 Select **Configure** > **Sites** from the menu.
The **Sites** list displays.
- 2 Select a site from the list. Select **Configure Site** > **Delete**.
The **Delete** dialog opens.
- 3 Select **OK** to delete the site, or select **Cancel** to cancel the action.

System Log Configuration

System Logging for Switches

Switches can be configured to stream system log messages to a local server. This option is configured at the site level. All of the switches in that site receive the same settings, either enable or disable, and the IP address and server port to which the system log messages will be forwarded. View the **Event Logs** tab by selecting **Sites** > **<siteName>** > **Event Logs**.

System Logging for Access Points

(ExtremeWireless WiNG Only) There is an *additional* system log option to include client events in system log files. This option applies to ExtremeWireless WiNG access points (APs) only, and becomes available when system log is enabled for an ExtremeWirelessWiNG site. System log for client events is useful for complying with the security requirements of some countries. This option is configured under **Advanced Settings** for a site. The clients event logs can be viewed, searched, and sorted on the individual AP page on the **Event Logs** tab. View the AP event logs tab by selecting **Devices** > **Access Points** > **wingApName** > **Event Logs**.

More Information

- [Configure a Site](#) on page 73
- [Configure Advanced Settings for Sites](#) on page 99

How to Enable Location Analytics

This topic describes a high level, end-to-end workflow about how to enable location analytics.

ExtremeCloud provides location analytics by integrating with ExtremeLocation.

All access points (APs) at a ExtremeCloud site can be configured to use ExtremeLocation. ExtremeCloud allows one device group per site.

To enable location analytics, follow this process:

- 1 [Configure the site's advanced settings to enable location analytics and configure the reporting interval.](#)

- For each location-supported AP at the site, configure the radio mode to sensor. The procedure differs, depending on whether you are [configuring ExtremeWireless](#) or [configuring ExtremeWireless WiNG](#).



Note

For some AP models, if the radio is not in sensor mode but it is serving ExtremeLocation, the AP can also be configured for either Promiscuous or Hop Off Channel modes. For information about which models support these advanced options, see the *Release Notes*.

- Select **Settings > General**, and enter the ExtremeLocation licensed account number in the **Extreme Location** pane.
- After you enable location analytics in ExtremeCloud, users can log in to ExtremeLocation directly from the ExtremeCloud user interface.

SNMP

SNMP is configured at the site level and is applied to all entitled switches and ExtremeWirelessWiNG APs in the site. It is disabled by default, but you can enable SNMPv2 or SNMPv3. When SNMP is enabled on a switch, all of the MIBs supported by the switch model can be accessed in read-only mode.



Note

For a list of the available MIBs, see the *EXOS User Guide*.

The configurable options that display depend on which mode you select. The SNMPv2 options are trap destinations and community strings. The SNMPv3 options are notification destinations (which must include an SNMPv3 user) and SNMPv3 users.

When you configure SNMPv3 options for one site, those options are available when you configure other sites.

SNMP access is read-only.

More Information

- [Configure a Site](#) on page 73
- [Configure Advanced Settings for Sites](#) on page 99

Wireless Intrusion Detection Services (WIDS)

Sites containing ExtremeWireless WiNG APs can enable Wireless Intrusion Detection Services (WIDS) at those sites. When enabled, the ExtremeWireless WiNG APs record the SSIDs and BSSIDs of the APs that they can see but which do not belong to the site. These can be the authorized APs of neighboring businesses or these can be unauthorized APs being used to penetrate the customer's network.

When an ExtremeWireless WiNG AP detects a BSSID that is not part of the site, it classifies the type of problem the foreign AP could represent. The problem can be as simple as the foreign AP is using bandwidth on the same channel as the authorized APs, or as serious as the discovery of a rogue AP. A rogue AP is an unauthorized AP connected to the customer's private network. While rogue APs are not always deployed with malicious intent, they always represent a major network security breach.

Two different WIDS detection options are available:

- **Enabled** - The AP performs detection only on the channel on which it is forwarding traffic.
- **Enabled with off-channel scan** - The AP performs detection on the channel it is serving and periodically will jump off of that channel to detect foreign APs on other channels. Service can be disrupted briefly when the AP scans off-channel.

The output of the WIDS scanning is visible in several places in the user interface. The event log for each site that has WIDS enabled contains events corresponding to various detections. The event log of the APs at the site that detected foreign APs will also contain events for those detections.

To view a list of all the foreign APs detected in the last 30 days, select **Devices > Unsanctioned APs**. Selecting on a row in the unsanctioned APs listing opens a page providing some details about the specific unsanctioned AP.

Unsanctioned APs are also included in the PCI compliance report.

10 Configuring Networks

Configure Network Services Configure Advanced Network Settings

Network services 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)

After your devices are registered, configure your network. We recommend configuring the default settings or creating new services (SSIDs) and roles to meet your specific needs.

The **Networks** page shows a list of your networks. Select a network from the list to configure or select **Add** to add a network.



Name	SSID	Status	Default Role	Privacy Type	Default VLAN
Staff	Staff	Enabled	Allow all	WPAv2 with PSK	Default
March19-NW1-3935	March19-NW1	Enabled	Allow all	WPAv2 with PSK	Default

Figure 71: Networks Page

When you select a network from the list:

- The network's **Dashboard** page opens and shows the statistical details.
- Using the tabs, you can access the sites, access points, switches, and clients that are associated with that network.
- The **Configure Network** button lets you edit the network configuration.

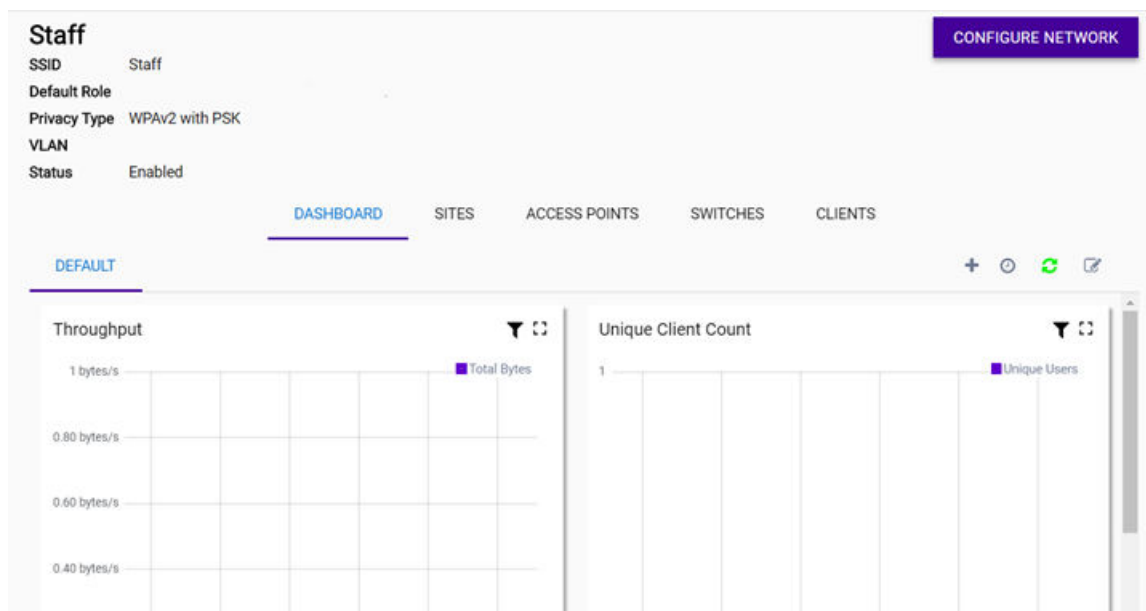


Figure 72: Individual Network Dashboard

More Information

- [Configure Network Services](#) on page 110
- [Configure Advanced Network Settings](#) on page 116

Configure Network Services

When you register devices for the first time, you use the configuration wizard to edit the default network (Staff). If you want to set up your own networks or make changes at any time, use this procedure.



Note

A maximum of 16 enabled SSIDs (eight per radio) can be assigned to a site.

For example, If you want to allow a completely open network, replace the default policy with a policy that allows traffic. You can use the predefined Allow All policy or create a more restrictive policy (the latter is recommended).

- 1 Select **Configure > Networks** from the menu.
The **Networks** list displays.
- 2 To add a new network, select **Add**. Alternatively, select an existing network, and then select **Configure Network**.

3 Edit the fields.

BACK

Network Name

SSID

Status

Auth Type

Captive Portal

Upon successful login redirect user to original destination

Default Role

Default VLAN

Note : (+) denotes IDENTIFI only attributes and (-) denotes WiNG only attributes

Figure 73: Configure Network

Network Name Enter any unique, user-friendly value that makes sense for your business. **Example:** Staff

SSID Enter a character string to identify the network. 32 characters maximum. Upper and lowercase allowed. **Example:** PermanentStaff

Status Choose an option:

Enabled This option turns on the network and leaves it on until you manually disable or delete it.

Disabled Disabling an network shuts off the service but does not delete it.

Schedule Scheduling lets you define specific periods when a service will be active.

AuthType Define the authorization type. You must [edit the privacy settings for WEP, WPAv2PSK, and WPA2 Enterprise w/ RADIUS](#).

Open Anyone can associate with the AP. This authorization type has no encryption and can use the Default Unauth role only.

WEP We do not recommend or endorse using WEP encryption due to the security flaws that are inherent with WEP. Access is allowed to any client that knows the pre-shared WEP key. WEP-64 uses a 40 bit key concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP 64 is a less robust

encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw. WEP-128 uses a 104 bit key which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP 128 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key.

WPAv2 with PSK	Access is allowed to any client that knows the pre-shared key. If MAC-based authentication (MBA) is also enabled, you can assign different roles to different devices with PSK. If MBA is not enabled, then devices with PSK use the Default Unauth role only. (TKIP encryption is available as an option with WPAv2 with PSK, but TKIP cannot be configured on its own. We do not recommend or endorse using TKIP due to the security flaws that are inherent with TKIP.)
WPA2 Enterprise w/ RADIUS	Supports 802.1x authentication with a RADIUS server, using AES encryption. All 802.1x protocols are supported. (TKIP-CCMP encryption is available as an option with WPAv2 Enterprise w/ RADIUS, but TKIP-CCMP cannot be configured on its own. We do not recommend or endorse using TKIP-CCMP due to the security flaws that are inherent with TKIP-CCMP.)
MAC-based Authentication	Select this option to enable MAC-based authentication with a RADIUS server, which restricts network access to specific devices by MAC address.
MBA Timeout Role	(For ExtremeWireless APs only) 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. If a moderately restrictive role is set (one allowing internet access but no local access), then clients can continue to function when the RADIUS server is unavailable.

- 4 If you enabled **WPA2 Enterprise w/ RADIUS** or **MAC-based Authentication** as the Auth Type, the **Configure RADIUS Servers** field displays. Select **Configure** and configure the fields in the **Configure RADIUS Servers** dialog.

Configure RADIUS Servers ?

Auth Type

Auth Type

Primary Server

IP Address

Shared Secret

Secondary Server

IP Address

Shared Secret

CLOSE

Figure 74: RADIUS Server Configuration

- Auth Type** Set the authentication protocol type for the RADIUS server (PAP, CHAP, MS-CHAP, or MS-CHAP2).
- IP Address** Enter a valid IP address for the RADIUS server. A primary IP address is required, and a secondary IP address is optional.
- Shared Secret** Enter the password that will be used between **ExtremeCloud** and the RADIUS server. If you are using a secondary IP address, you must provide a password for that IP address also.
- 5 (Optional) To enable a captive portal, select an option from the drop-down list. To use the built-in captive portal feature, select **Cloud**. To use a third-party or external captive portal, select **Other**. (If you have not yet configured the captive portal go to [How to Configure a Captive Portal](#) on page 182 and then return to this page to assign the portal to the network.) You can also enable the option to redirect the user to the original destination upon a successful login.
- If you selected **Cloud** or **Other**, the **Walled Garden DNS Whitelist** button displays.

- 6 (Optional) To enable a walled garden with the captive portal, select **Walled Garden DNS Whitelist**. Enter the Fully Qualified Domain Name (FQDN) names that you want to whitelist in the **Walled Garden DNS Whitelist** dialog. FQDNs can be full names (www.companyname.com) or partial names (companyname.com).




Partial FQDN matching is based on case sensitive suffix matching. For example, **companyname.com** will match companyname.com, www.companyname.com, xyz-abc.companyname.com or anything that ends with companyname.com.



Note

Select  to delete an FQDN.

These FQDNs are applied to the Unauth role assigned to the user, giving the user walled garden access to the specified FQDNs before they are authenticated.

- 7 Configure the default roles. Select  to create a new role or select  to edit an existing role. (You can also delete roles by selecting .)

Default Unauth Role Displays when the captive portal option is set to **Other**. Define a non-authenticated role that covers all traffic from devices that have not yet authenticated with the captive portal. Create a role with at least one rule that redirects at least some HTTP traffic (port 80, 8080, 443) to the captive portal web page. The role must allow DHCP and DNS traffic also. The role can allow other traffic. (This redirection is independent of the network's Authentication Type.) Only policies with redirection display in the drop-down list for this field.

Default Auth Role Displays when an external captive portal is enabled. Define an authenticated role.



Default Role Displays when captive portal is *not* enabled or when the **Cloud** captive portal is enabled. Define the access control role. This role is mandatory and covers all traffic from authenticated devices. The role filters network packets, either disallowing them or boosting the priority. Open, WPAv2PSK, and WPA2 Enterprise w/ RADIUS can use the Default Role, which is useful for simple deployments.


- 8 Create a new default VLAN or edit an existing VLAN. (You can delete unused VLANs.)



Note

If you are assigning an ExtremeCloud-created captive portal to a network that does not yet have an IP subnet to it, a pop-up **IP Subnet** dialog opens. You must provide an IP subnet for the captive portal to work.

Default VLAN The default VLAN is the VLAN on which the client traffic is placed by the AP if the policy assigned to the client does not explicitly place the client's traffic on a specific VLAN. In addition to the VLAN ID, the destination VLAN can be marked **Untagged**. (Complex deployments can attach to different VLANs simultaneously, but only one VLAN can be untagged.) Multicast filters can also be configured to control multicast forwarding to the wireless network. To edit multicast filters and the IP subnet, select  or  and then select **Advanced**.

- 9 (Optional) Specify the aggregate network bandwidth limit for the aggregate WLAN traffic on a per radio basis. Enabling this option prevents guest WLAN users from using more air time allowed by the WLAN rate limit. The allowed aggregate bandwidth limit is 128 - 2,500 Kbps. However, if you select , you can set the Class of Service to use an existing CoS, which makes the aggregate bandwidth unlimited, or configure CoS advanced settings for the priority, ToS/DSCP and mask.
- 10 (Optional) On the **Configure Network** page, select **Advanced to configure advanced settings**, such as admission control.

- 11 On the **Configure Network** page, select **Save**.

If you have created a new network (wireless SSID), you must then **add the network to a site** to start providing services to the wireless devices in that site.

Schedule Services

Scheduling lets you define the time for when a service is enabled. This can correspond to business hours or other criteria for security purposes. For example, you can automatically shut down a service during important events, such as final exams week, or for maintenance.

To schedule networks services:

- 1 In the **Status** field, select **Schedule**.
The **Set Schedule** button displays.
- 2 Select **Set Schedule**.
- 3 To change the timezone, select **Change**. Edit the timezone in the map, and select **Close**.
- 4 In the **Schedule** dialog, deselect the days that you do *not* want the services to run, or use the cursor to slide the time range and disable the service for a portion of a day.

Schedule ?

Select the days when the Service should be enabled and adjust the duration in the calendar

Timezone: America/New_York CHANGE

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Monday <input type="checkbox"/>	6am						
Tuesday <input type="checkbox"/>	7am						
Wednesday <input type="checkbox"/>	8am						
Thursday <input type="checkbox"/>	9am						
Friday <input type="checkbox"/>	10am						
Saturday <input type="checkbox"/>	11am						
Sunday <input type="checkbox"/>	12pm						
	1pm						

Figure 75: Schedule Services Configuration

- 5 Select **Close**.
You return to the **Configure Network** page.
- 6 Select **Save**.

Edit Privacy Settings

Privacy settings are editable for the WPAv2 with PSK and WPA2 Enterprise w/ RADIUS authorization types.

To edit network privacy settings:

- 1 In the **Auth Type** field, select **WPAv2 w/ PSK** or **WPA2 Enterprise w/RADIUS**.
Edit Privacy displays.

The screenshot shows a configuration form with the following fields and buttons:

- Network Name:** Service_1
- SSID:** Service_1
- Status:** SCHEDULE (dropdown) and SET SCHEDULE (button)
- Auth Type:** WPAV2 WITH PSK (dropdown) and EDIT PRIVACY (button, highlighted with a red box)

Figure 76: Edit Privacy Button

- 2 Select **Edit Privacy**.
The **Privacy Settings** dialog opens.
- 3 Set the privacy options as needed. The options that display depend on the Auth Type that you selected.

Protected Management Frames	Specifies the encryption status of 802.11 management frames: Enabled Uses encryption when possible. Disabled Disables encryption. Required Only accepts devices that can use management protected frames.
Fast Transition	(WPA2 Enterprise w/ RADIUS only) Enables fast transition for 11r enabled clients.
WPA Key	(WPAv2PSK only) Specify the WPA key (a shared key) using a text string.
WEP	We do not recommend or endorse using WEP encryption due to the security flaws that are inherent with WEP. Access is allowed to any client that knows the pre-shared WEP key. WEP-64 uses a 40 bit key concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP 64 is a less robust encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw. WEP-128 uses a 104 bit key which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP 128 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key.
TKIP and TKIP-CCMP	We do not recommend or endorse TKIP or TKIP-CCMP due to their inherent security flaws. Temporal Key Integrity Protocol (TKIP) encryption addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check and an extended initialization vector. However, TKIP also has vulnerabilities. (CCMP is a security standard used by the Advanced Encryption Standard (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a Message Integrity Check (MIC) using the proven Cipher Block Chaining (CBC) technique. Changing just one bit in a message produces a totally different result.)

- 4 Select **Close**.
You return to the **Configure Network** page.
- 5 Select **Save**.

Configure Advanced Network Settings

The default network settings are suitable for most deployments. If needed, you can fine tune those settings using the **Advanced Network Settings** dialog.

To configure the advanced network settings:

- 1 Select **Configure** > **Networks** from the menu.
The **Networks** list displays.
- 2 Select a network, and select **Configure Network**.
- 3 Select **Advanced**, and edit the fields.

Advanced Settings ?

Aggregate Network Bandwidth Limit

Redirect HTTPS

Hide SSID

Radio Management (11k) support

U-APSD (WMM-PS)

Use Admission Control for Voice (VO) *

Use Admission Control for Video (VI) *

Use Admission Control for Best Effort (BE) *

Use Global Admission Control for Background (BK) *

Client Roam Assist

Client To Client Communication

Enforce Client Load Balancing

Preauthenticated idle timeout (s) *

Postauthenticated idle timeout (s)

Maximum session duration (s)


Client IP Assignment

Classification

Note : (*) denotes IDENTIFI only attributes and (-) denotes WING only attributes

CLOSE

Figure 77: Advanced Network Settings For ExtremeWireless APs

Aggregate Network Bandwidth Limit	(For ExtremeWireless WiNG APs only) Specify the aggregate network bandwidth limit for the aggregate WLAN traffic on a per radio basis. Enabling this option prevents guest WLAN users from using more air time allowed by the WLAN rate limit. The allowed aggregate bandwidth limit is 128 - 2,500 Kbps. However, if you select  , you can set the Class of Service to use an existing CoS, which makes the aggregate bandwidth unlimited, or configure CoS advanced settings for the priority, ToS/DSCP and mask.
Redirect HTTPS	Forces all URLs on your web site to automatically redirect to the secure HTTPS version if an SSL certificate is installed.
Hide SSID	Prevents the SSID from going in a beacon message but sends out the SSID when a device probes the APs.
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.

(Dependent on the client's ability to support this option.) APs serving WLANs with 11k support enabled will perform a background scan to collect neighbor AP information and determine what alternative to recommend to the client.

U-APSD (WMM-PS) Improves your use of Power Save mode.



Caution

This option can interfere with device functionality.

Admission Control (For ExtremeWireless APs only) Enable one or more of these options to prioritize traffic and provide enhanced multimedia support. Improves the reliability of applications by preventing over-subscription of bandwidth. These thresholds are only applied to APs serving QoS-enabled WLANs that use Admission Control. The threshold limits are not configurable.

Admission Control for Voice (VO) Forces clients to request admission to use the high priority access categories in both inbound and outbound directions. **Default Thresholds:** this.maxVoiceAssocBw = 60; this.maxVoiceReassocBw = 80

Admission Control for Video Provides distinct thresholds for VI (video). **Default Thresholds:** this.maxVideoAssocBw = 40; this.maxVideoReassocBw = 60; this.reservedVideoBw = 20;

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. **Default Thresholds:** this.reservedNonAdmissBw = 20; this.maxBeAssocBw = 30; this.maxBeReassocBw = 40

Global Admission Control for Background (BK) Provides global admission control for background bandwidth. **Default Thresholds:** this.maxBkAssocBw = 20; this.maxBkReassocBw = 30;

Client Roam Assist (ExtremeWireless WiNG only) This option is specifically designed for legacy clients that do not roam, even when the signal strength is weak. When this option is enabled, APs can de-authenticate the client, forcing the client to associate with another access point. For clients that support 802.11v, the access point sends a transition packet instead of a de-authentication packet. It is up to the client to decide whether to roam away from the access point.

Client to Client Communication (ExtremeWireless WiNG only) When enabled, clients within a WLAN are allowed to exchange packets with each other. The disabled state only prevents clients within the WLAN from interoperating. The disabled state does not prevent clients on other WLANs from sending packets to this WLAN.

Enforce Client Load Balancing (ExtremeWireless WiNG only) Enable this option to provide load balancing for wireless client traffic.

Preauthenticated Idle Timeout (ExtremeWireless only) Set the number of seconds an idle session will timeout before a user authenticates, or use the default.

Postauthentication Idle Timeout Set the number of seconds an idle session will timeout after a user authenticates, or use the default.

Maximum Session Duration Set the maximum length of a session in seconds, or use the default.

Client IP Assignment (ExtremeWireless WiNG only) Assign one of the following options for client IP addresses:

Bridge Mode Wireless clients obtain their IP address from a DHCP server on the LAN to which the client joins.

NAT Mode The access point acts as a DHCP server and provides an IP address to the clients connecting to it. The access point in turn, NATs the traffic between the external network and the wireless clients.

Classification (ExtremeWireless WiNG only) Set the classification for Quality of Service (QoS) priority for the outgoing wireless network traffic flow.

Low Sets the traffic to low priority.

Normal Sets the traffic to normal priority.

Voice Assigns the outgoing wireless traffic to the Voice queue.

WMM For devices with Wi-Fi Multimedia (WMM) enabled, the standard provides multimedia enhancements for audio, video, and voice applications. WMM shortens the time between transmitting packets for higher priority traffic. WMM is part of the 802.11e standard for QoS. Some 802.11n client devices remain at legacy rates.

4 Select **Close**.

You return to the **Configure Network** page.

5 Select **Save**.

11 Configuring Access Points

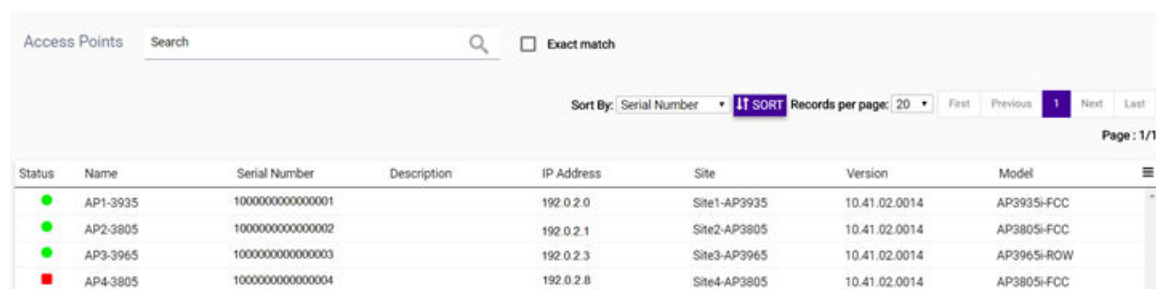
Dynamic Radio Management
Radios as Sensors
Configure ExtremeWireless Access Points
Configure ExtremeWireless WiNG Access Points
Configure Advanced Settings for an Access Point
Configure AP510e Professional Install Settings
Configure Advanced Radio Settings for AP5XX
Start Live Capture
Reboot an Access Point
Retrieve AP Trace Files
Upgrade AP3916ic

Extreme Networks access points (APs) use the 802.11 wireless standards (802.11a/b/g/n/ac) for network communications, and bridge network traffic to Ethernet LAN.

Supported access points can be managed by ExtremeCloud. For a list of supported devices, see the [ExtremeCloud Release Notes](#) or the [Hardware/Software Compatibility Matrices](#).

The **Access Points** page shows all of your access points (APs).

Select the menu icon (☰) to see the list of options for the page. You can specify the **Refresh** option, export some or all of the data to a CSV file, and configure which data columns display. By default, all columns display.



Status	Name	Serial Number	Description	IP Address	Site	Version	Model
●	AP1-3935	1000000000000001		192.0.2.0	Site1-AP3935	10.41.02.0014	AP3935i-FCC
●	AP2-3805	1000000000000002		192.0.2.1	Site2-AP3805	10.41.02.0014	AP3805i-FCC
●	AP3-3965	1000000000000003		192.0.2.3	Site3-AP3965	10.41.02.0014	AP3965i-ROW
■	AP4-3805	1000000000000004		192.0.2.8	Site4-AP3805	10.41.02.0014	AP3805i-FCC

Figure 78: Access Points Page

To configure the AP, select an AP from the list.

Sites containing ExtremeWireless WiNG APs can be configured to use Wireless Intrusion Detection Services (WIDS).

More Information

- [Configure a Site](#) on page 73
- [Wireless Intrusion Detection Services \(WIDS\)](#) on page 107
- [Configure ExtremeWireless Access Points](#) on page 122
- [Configure ExtremeWireless WiNG Access Points](#) on page 126

Dynamic Radio Management

When you modify the radio properties of an AP, the Dynamic Radio Management (DRM) features enable you to find the optimum radio configuration for your APs. DRM is enabled by default. The DRM:

- Adjusts transmit power levels to balance coverage between APs assigned to the same RF domain and operating on the same channel.
- Scans and coordinates with other APs to select an optimal operating channel.

The DRM feature consists of three functions:

- [Smart RF](#)
- [Dynamic Channel Selection \(DCS\)](#)
- [Auto Tx Power Control \(ATPC\)](#)

Smart RF

Self Monitoring at Run Time RF Management (Smart RF) simplifies radio frequency (RF) configuration. Smart RF also provides ongoing optimization of radio performance by allowing the APs to dynamically respond to changing RF conditions in real-time.

Smart RF is configured on a per site basis.

To configure a Smart RF policy, navigate to **Configure > Sites > RF Management**.

Dynamic Channel Selection (DCS)

DCS allows a Wireless AP to monitor traffic and noise levels on the channel on which the AP is currently operating. DCS can operate in two modes: Monitor and Active. DCS is not configurable. By default, Radio 1 is set to Monitor, and Radio 2 is set to Active.

Monitor When DCS is enabled in monitor mode and traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. The DCS monitor alarm is used for evaluating the RF environment of your deployed APs.

Active When DCS is enabled in active mode and traffic or noise levels exceed the configured DCS thresholds, the AP ceases operating on the current channel and uses ACS to find another channel to operate on. DCS does not trigger channel changes on neighboring APs.

Auto Tx Power Control (ATPC)

When enabled, ATPC provides your LAN with a stable RF environment by automatically adapting transmission power signals according to the coverage provided by the APs. When you disable ATPC, you are given the option of automatically adjusting the Max Tx Power setting to match the Current Tx Power Level.

ATPC is configured at the device level. To configure ATPC, select **Devices > Access Points**. Then select a device from the AP list, and select **Configure Device**. Under each radio, select **Advanced**.

More Information

- [Configure a Site](#) on page 73
- [Configure Advanced Settings for Sites](#) on page 99
- [Configure ExtremeWireless Access Points](#) on page 122
- [Configure ExtremeWireless WiNG Access Points](#) on page 126

Radios as Sensors

Some access points have the option to set the radio to Sensor mode. In Sensor mode, the radio does not service clients. Instead, the radio changes channels and functions as a sensor for ExtremeLocation, which enables the AP to report to ExtremeLocation. On some AP models, Sensor mode can co-exist with any radio mode, as the mode is configured per radio rather than per AP. The AP scans all channels that are allowed by the selected country.

Sensor mode is configured on individual access point radios, not at the site level.

More Information

- [Configure ExtremeWireless Access Points](#) on page 122
- [Configure ExtremeWireless WiNG Access Points](#) on page 126

Configure ExtremeWireless Access Points

You can modify settings for an ExtremeWireless access point (AP) and its radio attributes.

If you are using APs that have external antennas, the external antennas must be configured in the cloud user interface using the **Professional Install** dialog. The AP's LED status will default to **Identify** until the antennas are configured, and then you can change the LED status.

- 1 Select **Configure > Devices > Access Points** from the menu.
- 2 Select an AP from the **AP** list. Select **Configure AP**.

- 3 (Optional) Enter a name and a description.

The screenshot shows a configuration form with the following fields:

- Name:** Serial Number
- Description:** Main Floor Entry Access Point
- LED Status:** NORMAL (with a dropdown arrow)
- ADVANCED:** A button located below the LED Status field.

Figure 79: AP Configuration

- 4 Specify the LED status.

LED Status	Defines the type of LED behavior you want to use to follow the devices progress in registration.
Off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
Identify	This mode helps you identify a specific AP in case of any confusion. All LEDs blink simultaneously approximately two to four times every second. If this AP has external antennas, the Professional Install button displays and you must configure the antennas.
Normal	Identifies the AP status during the registration process during power on and boot process.

- 5 If the **Professional Install** button displays, you have registered an AP that has external antennas that must be configured before you can proceed to configure the AP radios. Select **Professional Install** to open the **Professional Install** dialog, edit the fields, and select **Close**.



Important

Only a professional wireless installer should configure the settings on this page.

The screenshot shows the Professional Install dialog with the following settings:

- Radio 1 Port 5G-1 Antenna Type:** NO ANTENNA
- Radio 1 Port 5G-2 Antenna Type:** NO ANTENNA
- Radio 2 Port 2.4G-1 Antenna Type:** NO ANTENNA
- Radio 2 Port 2.4G-2 Antenna Type:** NO ANTENNA
- Radio 1 attenuation:** 0
- Radio 2 attenuation:** 0
- CLOSE:** A button at the bottom right of the dialog.

Figure 80: Professional Install Dialog - ExtremeWireless AP

Antenna Type For each radio port, specify the antenna type. If the AP supports IoT, then you can set the IoT antenna type. An external antenna can be Indoor/Outdoor or Indoor only. (The antenna type is listed in the AP model's specifications.)

Radio Attenuation Specify the distance between access points in terms of signal attenuation, measured in decibels. (*Attenuation* is the reduction of signal strength during transmission. If the signal attenuates too much, it becomes unintelligible.) This value is used during channel assignment to minimize interference.

- 6 (Optional) [Configure the advanced settings](#), which include IoT overrides and RMA replacements.
- 7 Specify the radio attributes. When SmartRF is enabled, some attributes are configurable at the site level only.

Radios	Radio 5 Ghz	Radio 2.4 Ghz
Mode	ANC ▾	GN ▾
Admin Mode	ON ▾	ON ▾
Use SmartRF	YES ▾	YES ▾
Automatic Transmit Power Control *	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Channel Width	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Request new channel	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Max Tx Power [dBm]	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Channel Plan	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default

Note : (*) denotes IDENTIFI only attributes and (-) denotes WiNG only attributes

Figure 81: AP Radio Attributes Configuration



Note

Switching the mode or band causes the AP to reboot.

Mode Specify the radio mode for each radio. In [Sensor mode](#), the radio does not service clients. Instead, the radio functions as a sensor for ExtremeLocation, which enables reporting from the AP to ExtremeLocation. For some AP models, Sensor mode can co-exist with other radio modes. The available modes depend on the AP model. Mode can include: GN, ANC, BG, BGN, ANCX, SENSOR, GNX

Admin Mode Select **On** to enable or **Off** to disable this radio.

Use Smart RF Provides ongoing optimization of radio performance by allowing the APs to dynamically respond to changing radio frequency (RF) conditions in real-time. Select **On** to enable or **Off** to disable Smart RF. Smart RF is configured at the site level and applied to all APs that have been configured at the device level to use Smart RF.

Automatic Transmit Power Control Enable ATPC to provide a stable RF environment for a LAN by automatically adapting transmission power signals according to the coverage provided by the APs.

Channel Width Channel width helps to improve the effective throughput of the wireless LAN. Pick the channel mode that best suits the density of the deployment to avoid co-channel interference.

20 MHz Recommended for larger density deployments of greater than 10 APs.

40 MHz Recommended for deployments of 5 - 10 APs.

80 MHz Channel bonding is enabled. Recommended for deployments of less than five APs.

**Note**

The 160 MHz channel width is not supported for AP505 and AP510.

Auto Automatically switches between 20 MHz and 40 MHz, depending on how busy the extension channel is.

Request New Channel Specify the primary channel of the wireless AP. (If **Auto** is selected, the Auto-Channel Selection feature selects the primary channel.) Depending on the primary channel that is selected, channel bonding may be allowed upstream or downstream with an adjacent channel to increase throughput between devices.

**Note**

Channel plans are configured at the site level.

Max Tx Power Specify the maximum transmission power. The values are in dBm and vary by AP. The Max Tx Power should be set at a higher power level than the Min Tx Power.

- 8 Specify the Channel Plan options. The options that display depend on the radio's band (2.4 GHz or 5 GHz). If SmartRF is enabled, the settings for that radio are configurable at the site level.

Channel Plan If Smart RF is enabled on either radio, you can define a channel plan for the AP that limits which channels are available for use during an Smart RF scan. For example, you may want to avoid using specific channels because of low power, regulatory requirements, or radar interference.

All Channels	(5.0 GHz radios only) Scans all channels for an operating channel. Returns DFS and non-DFS channels, if available.
Custom Channels	When this option is selected, the Configure button displays and lets you configure individual channels from which the Smart RF selects an operating channel.
All Non-DFS Channels	(5.0 GHz radios only) Scans all non-DFS channels for an operating channel. This selection is always available, but if there are no DFS Channels available, the list is the same as the All Channels list.
3 Channel Plan	(2.4 GHz radios only) Scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in most other parts of the world.
4 Channel Plan	(2.4 GHz radios only) Scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in most other parts of the world.
Auto	Scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in most other parts of the world.

- 9 Select **View** to see the channel plan details.
- 10 On the **Configuration Details** page, select **Save**.
Your changes are applied and sent to the AP.

Configure ExtremeWireless WiNG Access Points

You can modify settings for a ExtremeWireless WiNG access point (AP) and its radio attributes.

- 1 Select **Configure > Devices > Access Points** from the menu.
- 2 Select an AP from the **AP** list. Select **Configure AP**.
- 3 (Optional) Enter a name and a description.

The screenshot shows a configuration form with the following elements:

- Name:** My WiNG Access Point
- Description:** (empty text box)
- LED Status:** NORMAL (dropdown menu)
- ADVANCED:** (button)

Figure 82: AP Configuration for Model with Sensor Mode

The screenshot shows a configuration form with the following elements:

- BACK:** (button)
- Name:** Wing-AP1-7562-WR
- Description:** (empty text box)
- LED Status:** NORMAL (dropdown menu)
- ADVANCED:** (button)
- PROFESSIONAL INSTALL:** (button)

Figure 83: AP Configuration for External Antenna Model

- 4 Specify the LED status.

LED Status	Defines the type of LED behavior you want to use to follow the devices progress in registration.
Off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
Identify	This mode helps you identify a specific AP in case of any confusion. All LEDs blink simultaneously approximately two to four times every second. If this AP has external antennas, the Professional Install button displays and you must configure the antennas.
Normal	Identifies the AP status during the registration process during power on and boot process.
- 5 If the **Professional Install** button displays, you have registered an AP that has external antennas that must be configured before you can proceed to configure the AP radios. Select **Professional Install** to open the **Professional Install** dialog, edit the fields, and select **Close**.



Important

Only a professional wireless installer should configure the settings on this page.

**Note**

For AP510e rules and settings, see [Configure AP510e Professional Install Settings](#).

Professional Install ?

	Radio 1	Radio 2
Antenna Gain	<input type="text" value="0"/>	<input type="text" value="0"/>
Environment	<input type="text" value="INDOOR"/>	<input type="text" value="INDOOR"/>

⚠ Only a professional wireless installer is authorized to change these settings.

Figure 84: Professional Install Dialog - ExtremeWireless WiNG AP

Antenna Gain For each radio (2.4 GHz and 5.0 GHz), set the antenna between 0.00 - 15.00 dBm. The **Auto** option lets the AP calculate the antenna gain. The access point's Power Management Antenna Configuration File (PMACF) automatically configures the access point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. **Default:** Auto

Antenna Type If the AP supports IoT, then you can set the IoT antenna type.

- 6 (Optional) [Configure the advanced settings](#), which include IoT overrides and RMA replacements.

7 Specify the radio attributes.

ADVANCED

Radios	Radio 1 - 2.4/5 GHz	Radio 2 - 5GHz
Mode	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> GN ▼ BGN GNX GN SENSOR BG ANC ANCX </div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> ANC ▼ </div>
Admin Mode		<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> ON ▼ </div>
Use SmartRF		<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> YES ▼ </div>
Automatic Transmit Power Control *	ⓘ SmartRF Policy of Site: Site1	ⓘ SmartRF Policy of Site: Site1
Channel Width	ⓘ SmartRF Policy of Site: Site1	ⓘ SmartRF Policy of Site: Site1
Request new channel	ⓘ SmartRF Policy of Site: Site1	ⓘ SmartRF Policy of Site: Site1
Max Tx Power [dBm]	ⓘ SmartRF Policy of Site: Site1	ⓘ SmartRF Policy of Site: Site1
	<div style="background-color: #4a4a8a; color: white; padding: 5px; display: inline-block;">ADVANCED</div>	<div style="background-color: #4a4a8a; color: white; padding: 5px; display: inline-block;">ADVANCED</div>

Figure 85: AP Radio Configuration



Note

Switching the mode or band causes the AP to reboot.

Mode	Specify the radio mode for each radio. In Sensor mode , the radio does not service clients. Instead, the radio functions as a sensor for ExtremeLocation, which enables reporting from the AP to ExtremeLocation. For some AP models, Sensor mode can co-exist with other radio modes. The available modes depend on the AP model. Mode can include: GN, ANC, BG, BGN, ANCX, SENSOR, GNX
Admin Mode	Select On to enable or Off to disable this radio.
Use Smart RF	Provides ongoing optimization of radio performance by allowing the APs to dynamically respond to changing radio frequency (RF) conditions in real-time. Select On to enable or Off to disable Smart RF. Smart RF is configured at the site level and applied to all APs that have been configured at the device level to use Smart RF.
Automatic Transmit Power Control	Enable ATPC to provide a stable RF environment for a LAN by automatically adapting transmission power signals according to the coverage provided by the APs.
Channel Width	Channel width helps to improve the effective throughput of the wireless LAN. Pick the channel mode that best suits the density of the deployment to avoid co-channel interference. <ul style="list-style-type: none"> 20 MHz Recommended for larger density deployments of greater than 10 APs. 40 MHz Recommended for deployments of 5 - 10 APs.

80 MHz Channel bonding is enabled. Recommended for deployments of less than five APs.



Note

The 160 MHz channel width is not supported for AP505 and AP510.

Auto Automatically switches between 20 MHz and 40 MHz, depending on how busy the extension channel is.

Request New Channel Specify the primary channel of the wireless AP. (If **Auto** is selected, the Auto-Channel Selection feature selects the primary channel.) Depending on the primary channel that is selected, channel bonding may be allowed upstream or downstream with an adjacent channel to increase throughput between devices.

- 8 Specify the Channel Plan options. The options that display depend on the radio's band (2.4 GHz or 5 GHz). If SmartRF is enabled, the settings for that radio are configurable at the site level.

Channel Plan If Smart RF is enabled on either radio, you can define a channel plan for the AP that limits which channels are available for use during an Smart RF scan. For example, you may want to avoid using specific channels because of low power, regulatory requirements, or radar interference.

All Channels (5.0 GHz radios only) Scans all channels for an operating channel. Returns DFS and non-DFS channels, if available.

Custom Channels When this option is selected, the **Configure** button displays and lets you configure individual channels from which the Smart RF selects an operating channel.

All Non-DFS Channels (5.0 GHz radios only) Scans all non-DFS channels for an operating channel. This selection is always available, but if there are no DFS Channels available, the list is the same as the All Channels list.

3 Channel Plan (2.4 GHz radios only) Scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in most other parts of the world.

4 Channel Plan (2.4 GHz radios only) Scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in most other parts of the world.

Auto Scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in most other parts of the world.

- 9 For supported AP5XX models, you can [configure advanced radio settings](#).

- 10 Select **Save**.

Your changes are applied and sent to the AP.

Configure Advanced Settings for an Access Point

This procedure is used for configuring an individual access point. (Advanced settings can also be [configured at the site level](#) and applied to all access points assigned to the site.)

To configure the advanced settings:

- 1 Select **Configure > Devices > Access Points** from the menu.
- 2 Select an AP from the **AP** list. Select **Configure AP**.

- Under the Name and Description fields, select **Advanced**.



Note

The **Advanced Settings** dialog for access points varies, depending on what type of access point is being configured.

Figure 86: AP Configuration for Model with Sensor Mode

Figure 87: AP Configuration for External Antenna Model

- (ExtremeWireless only) Edit the fields.

Figure 88: AP Advanced Settings

Link Aggregation Enable or disable the AP's L2 port association with a LAG (peer-to-peer) group.

Important



When configuring a LAG port for use by an ExtremeCloud-enabled access point, enable link aggregation on the access point first. If you do not do this, the AP can become isolated from the network. If the AP becomes isolated by the switch LAG port configuration, disable link aggregation on the switch ports used by the AP to allow the AP to join the network again. LAG can then be enabled on the AP, which takes one minute to update the configuration. Approximately two minutes later, LAG can be enabled on the corresponding switch ports.

Live Capture Lets an AP capture wired and wireless traffic and forward them to a remote Wireshark application.

Retrieve Traces Downloads trace files.

Reboot Restarts the device at the next synchronization interval, within five minutes.

Go to Traces Select this option to go directly to the downloaded log files for the device.

5 (ExtremeWireless WiNG only) Edit the fields.



Note

For AP5XX, see the following step.

Figure 89: ExtremeWireless WiNG Advanced Settings

Reboot Restarts the device at the next synchronization interval, within five minutes.

Configure Static IP Configure the VLAN mapping for this AP.

IP Address Specify the IP address that is assigned to the wireless client using this VLAN. Only IPv4 addresses are supported. Leave this field blank to allow DHCP assigned IP address for this VLAN.

Mask Specify the subnet mask in the xxx.xxx.xxx.xxx/xx format for this IP address.

Gateway Specify the gateway device to which traffic for the IP address is directed to.

DNS Server (Required) Enter the address of the site's DNS server. This is required for the topology set up and it is also required if you plan to use an external captive portal.

6 (AP5XX only) Edit the fields.

Advanced Settings ?

ACTIONS
OVERRIDES

Scan Mode CHANNEL LOCK ▾

Channels NONE SELECTED ▾

Link Aggregation DISABLED ▾

Advanced Operations REBOOT

Static IP


IP Address	Mask	Gateway	
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	🗑️

DNS Server +

RMA
CLOSE

Figure 90: AP5XX Advanced Settings

Scan Mode	Specify a scan mode
Default Scan	Specify this option to use the default channel list. This list includes all of the channels that the AP supports, and is optimized to scan with the widest possible channel. Radio 1 uses 2.4 Ghz and 5 Ghz (for AP510 only) channels. Radio 2 uses 5 Ghz channels.
Custom Scan	Specify a custom list of channels to scan from the drop-down list. When this option is selected, the Channels field displays. Radio 1 uses 2.4 Ghz and 5 Ghz (for AP510 only) channels. Radio 2 uses 5 Ghz channels. Channel width can also be specified for either or both radios.
Channel Lock	Specifies that the scan will be performed on only one channel. When this option is selected, the Channels field displays.
Channels	This field displays only when Channel Lock or Custom Scan is selected as the scan mode. Specify which channel the scan will be performed on, or specify Auto for automatic channel selection.

Link Aggregation	Enable or disable the AP's L2 port association with a LAG (peer-to-peer) group.
	<p>Important</p> <p> When configuring a LAG port for use by an ExtremeCloud-enabled access point, enable link aggregation on the access point first. If you do not do this, the AP can become isolated from the network. If the AP becomes isolated by the switch LAG port configuration, disable link aggregation on the switch ports used by the AP to allow the AP to join the network again. LAG can then be enabled on the AP, which takes one minute to update the configuration. Approximately two minutes later, LAG can be enabled on the corresponding switch ports.</p>
Reboot	Restarts the device at the next synchronization interval, within five minutes.
Configure Static IP	<p>Configure the VLAN mapping for this AP.</p> <p>IP Address Specify the IP address that is assigned to the wireless client using this VLAN. Only IPv4 addresses are supported. Leave this field blank to allow DHCP assigned IP address for this VLAN.</p> <p>Mask Specify the subnet mask in the xxx.xxx.xxx.xxx/xx format for this IP address.</p> <p>Gateway Specify the gateway device to which traffic for the IP address is directed to.</p> <p>DNS Server (Required) Enter the address of the site's DNS server. This is required for the topology set up and it is also required if you plan to use an external captive portal.</p>

- To set IoT overrides, select the **Overrides** tab. This option lets you override the IoT setting at the site level for this individual AP. All other APs assigned to the site will follow the site level settings. Select an option and enter a value in the corresponding text box. For more information about IoT settings, see [IoT Services](#) on page 101.

Advanced Settings ?

ACTIONS
OVERRIDES

IoT iBeacon Major	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>
IoT iBeacon Minor	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>
Eddystone URL	<input type="checkbox"/>	<input style="width: 95%;" type="text"/>

RMA
CLOSE

Figure 91: IoT Overrides Configuration

IoT iBeacon Major	Specify a subset of beacons within the larger UUID set. This value can represent a venue specific attribute, such as a specific store or a wing in a building. Values: 0 to 65635
-------------------	--

- IoT iBeacon Minor** Specify an individual beacon whose location you want to more precisely pinpoint. 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. **Values:** 0 to 65635
- Eddystone URL** Specify the URL that is included with the Eddystone-url beacon. **Limit:** 17 characters. The 17 characters does not include the protocol, but it does include the domain name. The URL is compressed, effectively allowing more than a 17 character input. See <https://github.com/google/edystone/tree/master/edystone-url> for the Eddystone-url compression rules to more accurately judge the length of your URL. If necessary, search for third-party URL shortening services available on the Internet.
- 8 For RMA Replacements, select **RMA**. This option copies the configuration from an existing device to the new, replacement device.
 - 9 Select **Close**.
You return to the **Configure AP** page.

Configure AP510e Professional Install Settings

AP510e access points have external antennas with the following rules that apply to the 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 and 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 sensor and Radio 2 forwards traffic.
 - Radio 2 is enabled only if one or more antennas are configured in Group 1.
 - Radio 1 – sensor needs one or more antennas configured in 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.
- 1 Select **Configure > Devices > Access Points** from the menu.
 - 2 Select **Professional Install** (this button only displays for APs that have external antennas).
 - 3 Edit the fields in the **Professional Install** dialog.



Important

Only a professional wireless installer should configure the settings on this page.

Advanced (Radio 1 - 2.4GHz) ?

OCS Channels NONE SELECTED ▾

OCS Interval (dtims) 20

CLOSE

Figure 92: Professional Install Dialog - AP510e

Antenna Type	For each radio port, specify the antenna type. If the AP supports IoT, then you can set the IoT antenna type. An external antenna can be Indoor/Outdoor or Indoor only. (The antenna type is listed in the specifications for the AP model.)
Radio Attenuation	Specify the distance between access points in terms of signal attenuation, measured in decibels. (Attenuation is the reduction of signal strength during transmission. If the signal attenuates too much, it becomes unintelligible.) This value is used during channel assignment to minimize interference.

- 4 Select **Close**.

Configure Advanced Radio Settings for AP5XX

Off-Channel Scanning (OCS) settings are available for supported AP5XX models. Smart RF relies on 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. The advanced radio settings help you improve data packet throughput by defining the channels that will participate in OCS and configure the intervals.



Note

For a list of supported APs, see the *Release Notes*.

To configure advanced radio settings for AP5XX:

- 1 Select **Configure** > **Devices** > **Access Points** from the menu.
- 2 Select an AP from the **AP** list. Select **Configure AP**.

- 3 Select **Advanced** under each radio. This option does *not* display when the radio mode is set to Sensor.

Radios	Radio 1 - 2.4/5 GHz	Radio 2 - 5GHz
Mode	ANCX ▾	ANCX ▾
Admin Mode	ON ▾	ON ▾
Use SmartRF	YES ▾	YES ▾
Automatic Transmit Power Control	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Channel Width	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Request new channel	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Max Tx Power [dBm]	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
Channel Plan	SmartRF Policy of Site: Default	SmartRF Policy of Site: Default
	ADVANCED	ADVANCED

Figure 93: AP Radio Configuration

- 4 In the **Advanced** dialog, set the Off-Channel Scanning (OCS) options.

Advanced (Radio 1 - 2.4GHz) ?

OCS Channels NONE SELECTED ▾

OCS Interval (dtims) 20

CLOSE

Figure 94: Advanced Radio Settings for AP 5XX

OCS Channels Use the drop-down list to define a 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) Set the OCS interval to a value between 2 -100 dtims.

- 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)
- 5 Select **Close**.
You return to the **Configure AP** page.
 - 6 Select **Save**.
Your changes are applied and sent to the AP.

Start Live Capture

An ExtremeWireless access point (AP) can capture wired and wireless traffic and forward it to a remote Wireshark application. This feature, called Live Capture, must be enabled on the AP using ExtremeCloud.

- 1 Make sure that the Wireshark application is running on a host that has access to the capturing AP's wired Ethernet interface. Wireshark must be configured to capture packets from a remote interface. Consult Wireshark documentation to configure the application to listen on a Remote Interface.
- 2 From the left menu, select **Configure > Devices > Access Points**.
- 3 Select the ExtremeWireless capturing AP from the list of devices.
The individual AP page opens.
- 4 Select **Configure AP > Advanced**.
- 5 In the **Timeout** field, specify a timeout duration, and then select **Live Capture**.

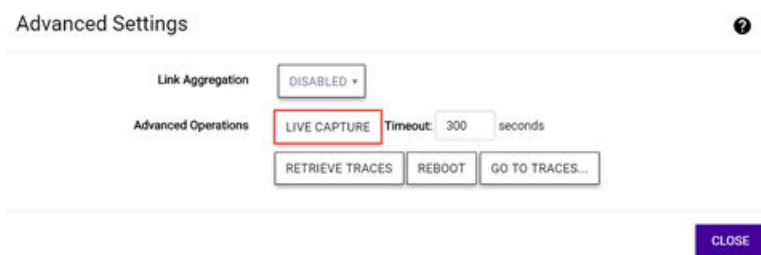


Figure 95: AP Advanced Settings

A message displays stating that Live Capture has started.

Reboot an Access Point

Remotely rebooting a cloud-managed AP when the APs LED status shows faulty operation or the AP is down.

When an access point (AP) LED status shows faulty operation or a dashboard report shows that the AP is down, you can reboot the AP device remotely.



Note

If your AP continues to have problems after rebooting, contact Support to see if resetting the AP to its factory defaults is appropriate.

- 1 Select **Configure > Devices > Access Points** from the menu.

- 2 Select an AP.
- 3 Select **Configure AP > Advanced**.
The options that display depend on the type of AP that you are configuring.
- 4 Select **Reboot**.
The device reboots at the next synchronization interval, within five minutes.

Retrieve AP Trace Files

You can download trace files to send to Support for help with troubleshooting for an access point (AP).



Note

Trace files expire after 24 hours.

- 1 Select **Configure > Devices > Access Points** from the menu.
- 2 Select an access point from the list.
- 3 Select **Configure AP > Advanced**. The options that display depend on the AP model.
- 4 Select **Retrieve Traces**.
The traces are downloaded.
- 5 When prompted, select **Go to Traces**.
The **Traces** tab automatically opens for the device and you can view the trace files in the user interface.

Upgrade AP3916ic

This topic describes the upgrade process that takes place for the ExtremeWireless AP3916ic access point (AP). This process takes place automatically and is described here for edification.

- 1 When an upgrade is required, **ExtremeCloud** responds to the access point (AP) check-in with an Upgrade action.
- 2 The Upgrade action can contain one or two software versions to which AP should upgrade. If there are two upgrade entries, one entry is for the camera. If the response requires both AP and camera software upgrades, the AP ignores the camera firmware upgrade request.
- 3 The AP upgrades its own firmware, just like any other cloud-enabled AP.
- 4 The AP reboots, and then sends a connect request.
- 5 When the connect request is acknowledged, the AP sends an upgrade query. **ExtremeCloud** determines that the AP is running the correct AP software but the wrong camera software. (Cloud-management considers the wrong camera as a failure).
- 6 **ExtremeCloud** retries the upgrade by responding with the new camera software version.
- 7 The AP receives the camera software version, downloads it, and then upgrades the camera to the software.
- 8 The AP reboots after the camera software upgrade, and then sends a connect request to the **ExtremeCloud**.
- 9 When **ExtremeCloud** responds to the connect request, the AP sends an upgrade query.

- 10 **ExtremeCloud** detects that the AP is running the correct versions of the AP and camera software, and then allows the AP to request configuration.
- 11 The AP configuration is updated and goes back into service.

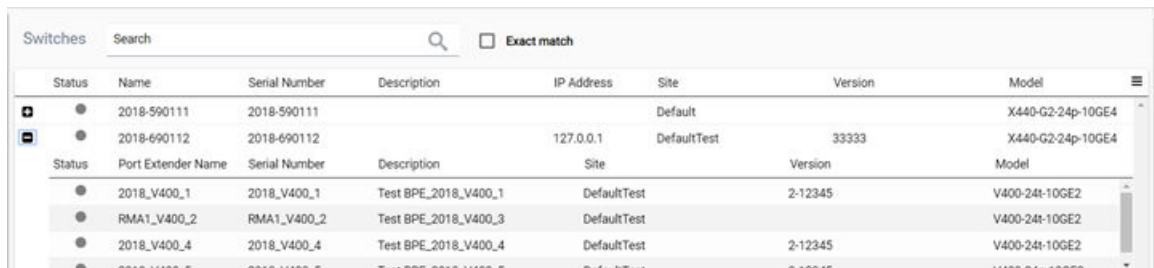
12 Configuring Switches

LLDP Mode
Multiple Spanning Tree Protocol
Configure a Switch
View the PoE Budget
LAG Ports
MLAG
Configure an Individual Port
CLI Mode

Supported ExtremeSwitches and Extended Edge Switches can be managed by ExtremeCloud. For a list of supported devices, see the [ExtremeCloud Release Notes](#) or the [Hardware/Software Compatibility Matrices](#).

The **Switches** page shows all of your entitled switches. You can select a switch from the list to configure.

Select the menu icon (☰) to see the list of options for the page. You can specify the **Refresh** option, export some or all of the data to a CSV file, and configure which data columns display. By default, all columns display.



Status	Name	Serial Number	Description	IP Address	Site	Version	Model
+	2018-590111	2018-590111			Default		X440-G2-24p-10GE4
+	2018-690112	2018-690112		127.0.0.1	DefaultTest	33333	X440-G2-24p-10GE4
Status	Port Extender Name	Serial Number	Description	Site	Version	Model	
	2018_V400_1	2018_V400_1	Test BPE_2018_V400_1	DefaultTest	2-12345	V400-24t-10GE2	
	RMA1_V400_2	RMA1_V400_2	Test BPE_2018_V400_3	DefaultTest		V400-24t-10GE2	
	2018_V400_4	2018_V400_4	Test BPE_2018_V400_4	DefaultTest	2-12345	V400-24t-10GE2	
	2018_V400_5	2018_V400_5	Test BPE_2018_V400_5	DefaultTest	2-12345	V400-24t-10GE2	

Figure 96: Switches Page

If a switch has a plus sign (⊕) in front of it, it is a controlling bridge. Expand the list to see the list of BPE switches in the VPEX.

To edit the switch, select a switch from the list.

More Information

- [Configure a Switch](#) on page 142

LLDP Mode

The Link Layer Discovery Protocol (LLDP) is defined by IEEE standard 802.1ab and provides a standard method for discovering physical network devices and their capabilities within a given network management domain. LLDP-enabled network devices include access points and bridges, and LLDP enables these devices to:

- Advertise device information and capabilities to other devices in the management domain.
- Receive and store device information received from other network devices in the management domain.

LLDP-discovered information provides device information to SNMP (Simple Network Management Protocol) to ExtremeCloud, which can present the information in reports and topology maps.

When a switch is configured by ExtremeCloud, LLDP Receive and LLDP Transmit modes are automatically enabled on all ports.

The LLDP PDU is not configurable in ExtremeCloud.

More Information

- [Configure a Switch](#) on page 142
- [Configure an Individual Port](#) on page 152

Multiple Spanning Tree Protocol

Multiple Spanning Tree Protocol (MSTP), based on IEEE 802.1Q-2003 (formerly known as IEEE 802.1s), allows the bundling of multiple VLANs into one spanning tree topology.

MSTP logically divides a Layer 2 network into regions. Each region has a unique identifier and contains multiple spanning tree instances (MSTIs). An MSTI is a spanning tree domain that operates within and is bounded by a region. MSTIs control the topology inside the regions. The Common and Internal Spanning Tree (CIST) is a single spanning tree domain that interconnects MSTP regions. The CIST is responsible for creating a loop-free topology by exchanging and propagating BPDUs across regions to form a Common Spanning Tree (CST).

MSTP treats each switch as its own region, identified by the switch's MAC address. A single Common and Internal Spanning Tree (CIST) is built across all of your sites.

ExtremeCloud-enabled switches implement standard MSTP for network loop protection. By default, MSTP is disabled but can be enabled in the **Administration** section of the user interface. Enabling MSTP enables it on all of the cloud-enabled switches in a ExtremeCloud-enabled network.

The bridge priority for switches is set to defaults that are based on the switch model. These defaults are selected to discourage cloud-enabled switches from becoming the root of a spanning tree. More powerful cloud-enabled switches are assigned priorities that will cause them to be more likely to be selected as a spanning tree root node than a pure edge switch. However, the defaults can be overridden.

Port is automatically classified as **edge** if the port's function is set to AP or Host. Edge-Safeguard and BDPU-Restrict (or BDPU Guard) are applied to edge ports automatically. If a port's function is inter-

switch, the port is classified as point-to-point and loop protect (or loop guard) is applied. For more information about these Extreme EXOS features, see the EXOS documentation at <http://extremenetworks.com/support/documentation>.

More Information

- [Configure a Switch](#) on page 142
- [Configure General System Settings](#) on page 224

Configure a Switch

As an administrator, you can make changes to your switch configuration. Use this procedure to configure an ExtremeSwitch or an Extended Edge Switch

Some use cases include:

- Deploying a cloud-enabled ExtremeSwitch
- Deploying a new collection of cloud-enabled APs and switches
- Deploying a new service that uses a new VLAN
- Enabling LAG to an AP
- Diagnosing and correcting a connectivity issue
- Rebooting a switch
- Cloning a configuration for an RMA replacement

When a configuration change is made, it gets pushed to the switch the next time the switch checks in with **ExtremeCloud**. If the switch does not receive a response from **ExtremeCloud**, the switch reboots and loads the previous working configuration that is stored on the switch.



Note

Most switch management is done using the graphical user interface (GUI). **ExtremeCloud** also offers a [CLI mode](#) option.

To configure a switch:

- 1 Select **Configure > Devices > Switches** from the menu.
- 2 Select a switch from the list.
Details about the switch are displayed. ([The PoE budget can be viewed in the Hardware pane.](#))
- 3 Select **View Configuration**.

- 4 Edit the fields:

The screenshot shows a configuration page for a switch. At the top, there are buttons for 'ADVANCED' and 'SAVE'. The 'Name' field contains '1647G-00282' and the 'Description' field contains '200SeriesOS 220-24t-10GE2'. Below this is a table of ports for LAG configuration:

LAG	Admin State	Name	Alias	Function	Speed	Neighbor	lagmembers
<input checked="" type="checkbox"/>	On	1/0/17	17	Other	0		
<input type="checkbox"/>	On	1/0/18	18	Other	0		
<input type="checkbox"/>	On	1/0/19	19	Other	0		
<input type="checkbox"/>	On	1/0/20	20	Other	0		
<input type="checkbox"/>	On	1/0/21	21	Other	0		
<input type="checkbox"/>	On	1/0/22	22	Other	0		
<input type="checkbox"/>	On	1/0/23	23	Other	0		
<input type="checkbox"/>	On	1/0/24	24	Other	0		
<input type="checkbox"/>	On	1/0/25	25	Other	10 Gbps		
<input type="checkbox"/>	On	1/0/26	26	Other	10 Gbps		

At the bottom, there is a 'NEW LAG' dialog box with the text 'Set the selected ports' and two dropdown menus: 'ADMIN STATE' (set to 'OFF') and 'to' (set to 'OFF'). An 'APPLY' button is also present.

Figure 97: Switch Configuration

Name (Required) Specify a unique name.

Ports Enable the check box to perform bulk configuration of ports, or select a single port from the list to configure.

Set Selected Ports Select one or more ports from the list. Then, one at a time, set the **Admin State**, **Port Function**, and **PoE** options to **On** or **Off**. Select **Apply** after each selection.

- 5 Select **New LAG**. Edit the fields (the dialog displays the options when you select a master port) and select **Save Master Port**. You can either create or delete LAG ports. Link aggregation allows multiple physical ports to be aggregated into one logical port, or link aggregation group (LAG), which provides increased bandwidth and link redundancy.

Important



When configuring a LAG port for use by an ExtremeCloud-enabled access point, enable link aggregation on the access point first. If you do not do this, the AP can become isolated from the network. If the AP becomes isolated by the switch LAG port configuration, disable link aggregation on the switch ports used by the AP to allow the AP to join the network again. LAG can then be enabled on the AP, which takes one minute to update the configuration. Approximately two minutes later, LAG can be enabled on the corresponding switch ports.

LAG Configuration ?

Choose a Master Port:

Master Port 5

▲
Drag-and-drop

Ports eligible for LAG membership

1	2	3	4	6	7	8	9	10	11	12	13
14	15	16	17	18	19	20	21	22	23	24	25
26	27	28									

Figure 98: LAG Configuration

Choose a Master Port Specify the master port for the LAG configuration on this switch by selecting from the drop-down list. Then drag and drop the ports you want into the **Master Port** pane.

- 6 Select **Advanced**. Select the options you want, and select **Close**.



Note

LLDP is automatically enabled on the switch and is not configurable. The **RMA** button is used for RMA replacements. For more information, see [RMA Replacement Process](#) on page 40.

Advanced Settings ?

Bridge Priority

IGMP snooping

- STP is configured globally. [Click here](#) to configure STP
- VLANs are configured under Policy. [Click here](#) to manage VLANs.
- SNMP is configured under Site. [Click here](#) to go to the Site.

Figure 99: Switch Advanced Settings

Bridge Priority By configuring the STPD (Spanning Tree Domain) bridge priority, you change the likelihood of the switch becoming the root bridge. The lower the numerical value of the priority, the more

likely the switch is the root bridge. Multiples of 4,096 are used to determine the bridge priority, per the 802.1D-2004 standard. **Default:** Depends on the switch model.



Important

You should not configure this STP parameter unless you have considerable knowledge and experience with STP. The default parameter is adequate for most networks.

IGMP Snooping	Enable snooping of Internet Group Management Protocol (IGMP) to provide a method for intelligently forwarding multicast packets within a Layer 2 broadcast domain. By <i>snooping</i> 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
LED Status	Select On to make the LEDs flash on the switch. Can be used for identifying a switch in a DC or a rack or for testing the communication between the switch and cloud management. Stays on until turned off. Default: Off
Change to CLI-Mode	Manage the switch in CLI mode directly from the cloud user interface. Review the CLI-Mode documentation before selecting this option.
Reboot	Restarts the switch.
RMA	Lets you replace this device with a new device and automatically assign the configuration to the new device.
Clone From	Use this option with an RMA switch replacement. This options lets you clone the configuration from the old switch to the new replacement switch.

- If needed, configure STP, VLANs, and SNMP by selecting the corresponding links in the **Advanced Settings** dialog.
- In the **Advanced Settings** dialog, select **Close**.
- On the **Configure Switch** page, select **Save**.

View the PoE Budget

By default, ExtremeCloud enables PoE on all switch ports for switches that support PoE. Not all switch models have enough power to support 802.3at on every port.

An estimator is provided at the switch level that shows the maximum number of each AP type that the switch can power with the remaining PoE budget. The calculation is conservative and assumes the maximum power that can be drawn on all devices.

To view the PoE budget estimation:

- Select **Configure > Devices > Switches** from the menu.
- Select a switch from the list.

Details about the switch are displayed.

- 3 In the **Hardware** pane, next to **PoE Budget**, select the **i** button to display the **PoE Budget AP Estimator**. (This button only displays if the switch supports PoE.)



Note

This estimator is only available if the switch supports PoE.

PoE Budget AP Estimator

Given the current PoE power draw on the switch, additional APs could be added as follows:

AP Model	Max Draw (Watts)	Total AP Capacity	AP Capacity Remaining
AP3935	25	13	4
AP3965	25	13	4
AP3805	15	22	8
AP3912	12.7	26	9
AP3912 with PoE Client (PSE)	24	13	5
AP7502	6.5	48	18
AP7522	13.4	24	9
AP7532	15	22	8
AP7562	17	19	7

CLOSE

Figure 100: PoE Budget AP Estimator

Next, you can enable or disable PoE on a port. This step is optional.

LAG Ports

Link Aggregation Overview

Link aggregation (also known as load sharing) lets you increase bandwidth and availability by using a group of ports to carry traffic in parallel between switches.

A Link Aggregation Group (LAG) allows multiple physical switch ports to be aggregated into one logical port, which provides the advantages of:

- Increased bandwidth when the egress bandwidth of traffic exceeds the capacity of a single link.
- Multiple links (link redundancy) for the purpose of network resiliency.

In both situations, the aggregation of separate physical links into a single logical link multiplies the total link bandwidth, in addition to providing resiliency against individual link failures.



Note

All ports in a LAG must run at the same speed and duplex setting.

If a port in a LAG fails, traffic is redistributed to the remaining ports in the LAG. If the failed port becomes active again, traffic is redistributed to include that port.



Note

Load sharing must be enabled on both ends of the link, or a network loop may result.

How LAGs Work with **ExtremeCloud**

As an administrator, you can configure a LAG port on a switch. 1-N ports can be selected. N is a function of the switch. All ports assigned to a LAG must have the same function (AP port, uplink port, host port, or other port).

LAG configuration does not create a new port. Instead, one port is assigned as the master port and receives all of the configuration, and the configuration applies to all of the LAG members. Adding a port to a LAG deletes out its previous configuration, and the port will inherit the LAG configuration.

If the port function of the LAG is access point (AP), you cannot assign more than two ports to the LAG.

Important



When configuring a LAG port for use by an **ExtremeCloud**-enabled access point, enable link aggregation on the access point first. If you do not do this, the AP can become isolated from the network. If the AP becomes isolated by the switch LAG port configuration, disable link aggregation on the switch ports used by the AP to allow the AP to join the network again. LAG can then be enabled on the AP, which takes one minute to update the configuration. Approximately two minutes later, LAG can be enabled on the corresponding switch ports.

If you want to configure a port differently than the LAG or assign it to a different LAG, you must remove the port from the existing LAG.

More Information

- [Configure a Switch](#) on page 142
- [Configure an Individual Port](#) on page 152

View LAG Port Details

To view LAG port memberships for a switch and view to details:

- 1 Select **Configure** > **Devices** > **Switches** from the menu.
- 2 Select a switch from the list.
Details about the switch are displayed, along with a series of tabs including **Dashboard**, **winPorts**, **LAG Ports**, **Networks**, **Event Logs**, and **Traces**
- 3 Select **LAG Ports**.
The **LAG Ports** tab opens and displays information about the Master and LAG Member ports, including names, aliases, ports speeds, status, function, and so on.
- 4 (Optional) Select the menu icon (☰) to export data and manage which columns display in the user interface.

MLAG

The MLAG feature allows you to combine ports on two switches to form a single logical connection to another network device. The other network device can be either a server or a switch that is separately configured with a regular LAG (or appropriate server port teaming) to form the port aggregation.

Note



If there is already an MLAG configuration on the switch before connecting to **ExtremeCloud**, the MLAG becomes a configuration of the **ExtremeCloud**. Thereafter, any changes to the MLAG configuration must be applied only from the **ExtremeCloud** - you cannot do MLAG configuration changes directly on the switch.

The following diagram displays the elements in a basic MLAG configuration:

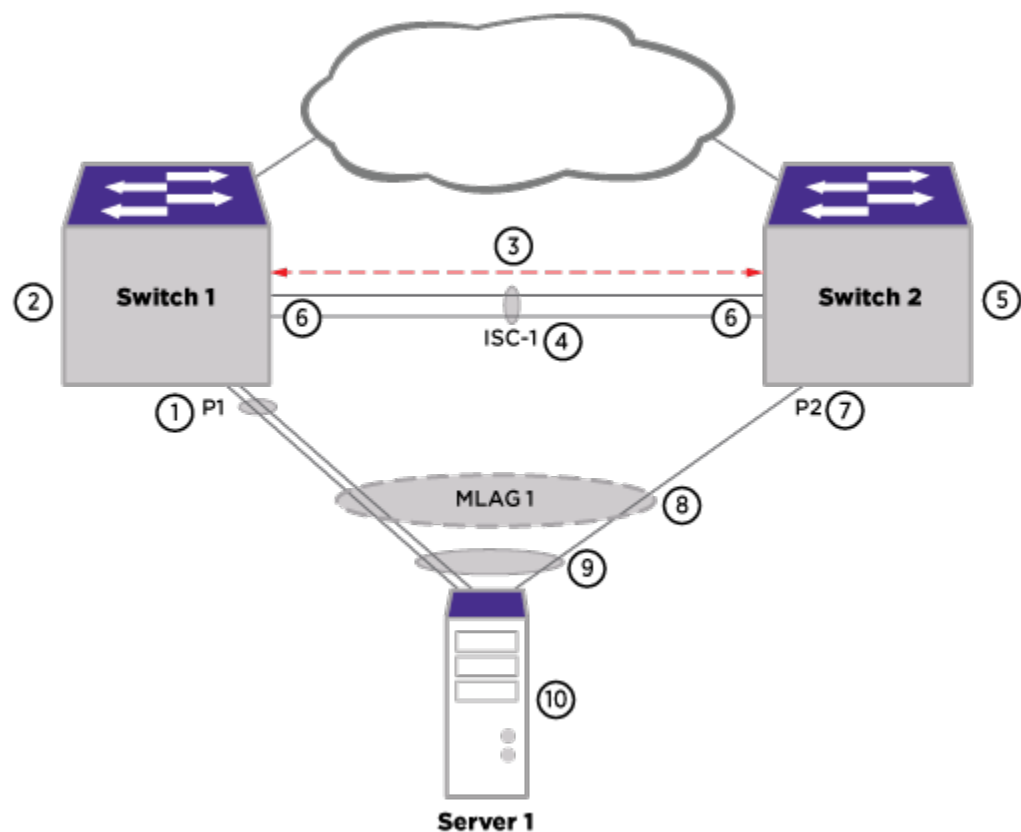


Figure 101: MLAG Elements

- 1 MLAG port that is a load-shared link. This port is the peer MLAG port for <Switch2:Port P2>.
- 2 MLAG peer switch for Switch 2.
- 3 Inter-switch connection (ISC or ISC VLAN) has only the ISC port as a member port on both MLAG peers.
- 4 ISC link that connects MLAG peers.
- 5 MLAG peer switch for Switch 1.
- 6 ISC ports.
- 7 MLAG port that is a non-load-shared link. This port is the peer MLAG port for <Switch1:Port P1>.

- 8 MLAG group (MLAG-ID 1) that has two member ports (one load-shared and one non-load-shared member).
- 9 MLAG remote node sees the MLAG ports as regular load-shared link.
- 10 MLAG remote node - can be a server or a switch.

The operation of this feature requires two ExtremeXOS switches interconnected by an Inter-Switch connection (ISC). The ISC is a normal, directly connected, Ethernet connection and it is recommended that you engineer reliability, redundancy where applicable, and higher bandwidth for the ISC connection. Logically aggregate ports on each of the two switches by assigning MLAG identifiers (MLAG-ID). Ports with the same MLAG-ID are combined to form a single logical network connection. Each MLAG can be comprised of a single link or a LAG on each switch. When an MLAG port is a LAG, the MLAG port state remains up until all ports in the LAG go down.

As long as at least one port in the LAG remains active, the MLAG port state remains active. When an MLAG port (a single port or all ports in a LAG) fails, any associated MAC entries are moved to the ISC, forcing traffic destined to the MLAG to be handled by the MLAG peer switch. Additionally, the MLAG peer switch is notified of the failure and changes its ISC blocking filter to allow transmission to the MLAG peer port. In order to reduce failure convergence time, you can configure MLAG to use ACLs for redirecting traffic via the "fast" convergence-control option.

Each of the two switches maintains the MLAG state for each of the MLAG ports and communicates with each other to learn the MLAG states, MAC FDB entries, and IP multicast entries of the peer MLAG switch.

MLAG Peer Prerequisites and Impacts

MLAG Prerequisites

In **ExtremeCloud**, MLAG peers must:

- Be the same hardware model
- Use the same software version, except during an upgrade
- Have the same licenses
- Have a network path to **ExtremeCloud**
- Already be grouped together with a LAG (peers communicate using Ethernet)

MLAG Impacts

The following table shows additional MLAG assumptions that are specific to other protocols and features when using **ExtremeCloud**:



Note

To function properly, MLAG peers should run the same version of ExtremeXOS.

Table 13: MLAG Impacts with ExtremeCloud

Item	Impact
Site	Two MLAG peers must be in the same site.
LLDP	LLDP is used to verify that two MLAG peers have a direct link.
Link-Local IP address	The IP address for MLAG peers is a Link-Local IP address (169.254.x.x).
ISC VLAN	This item is auto-generated by CE and is read-only in the user interface.
vlanId	Is generated from 4089 down and is not used for both peers.
malgId	This item is auto-generated by CE and is read-only in the user interface.
mLagPeerIpAddress	This item is auto-generated by CE and is read-only in the user interface.
mLagPeerNetMask	This item is auto-generated by CE and is read-only in the user interface.
ISC port	A new port type that functions similarly to an Interswitch port.

MLAG Deployment

The following MLAG deployment use cases are supported and handled in the manner described in each section.

Two Newly Deployed Switches

In this use case, the switches are all newly deployed. Follow this process to deploy MLAG on the switches:

- 1 Physically install the two switches and connect them to each other.
- 2 Make sure that ztpstack is not running on the switches.
- 3 Connect the switches to **ExtremeCloud**. After the two switches check in, **ExtremeCloud** detects that two switches are connected to each other and verifies that they meet the prerequisites to be MLAG peers. A notification is created.
- 4 Log in to **ExtremeCloud**. Look for the notification in the alert bell in the upper right corner of the user interface. The notification states that MLAG peer candidates have been found and lets you configure MLAG peers on optimally selected ports.
- 5 Select the link in notification to go to the **Add MLAG** page. [Configure the MLAG](#).

One Existing Switch and One Newly Deployed Switch

If you already have one switch connected to **ExtremeCloud** and are deploying a new switch, you will not get a notification. Instead, manually navigate to the page where you will [configure the MLAG](#).

Add a Port on Each Peer to an MLAG

In this deployment use case, a pair of switches have already been configured as MLAG peers. Both peers are operational. A new VPEX switch has been cabled to each peer of the MLAG peer.



Note

A variation on this use case is that if the ISC link is already set up, the VPEX switch and the MLAG pair will be detected. You will see notification in the user interface that lets you configure MLAG peers on optimally selected ports.

To add a port to each MLAG peer:

- 1 From the left menu, select **Devices > MLAG**.
- 2 From the list of existing MLAG peers, select the one you want to configure.
- 3 Select one port or a list of ports on each of MLAG peer.
- 4 Select Save. The MLAG ports are saved to a LAG if they are not already LAG port. The MLAG is created and the MLAG port is enabled.

Detect When Switches Coming Under Management Have MLAG Enabled Already

In this use case, you already have MLAG peer switches in your environment (the ISC links and MLAG ports have already been configured by you or by a script such as ztpstack). When you add these existing MLAG peer switches to **ExtremeCloud** orchestration, Topology Manager detects and imports the existing MLAG instance to **ExtremeCloud**.

Configure an MLAG

The MLAG feature allows you to combine ports on two switches to form a single logical connection to another network device. The other network device can be either a server or a switch that is separately configured with a regular LAG (or appropriate server port teaming) to form the port aggregation.



Note

If there is already an MLAG configuration on the switch before connecting to **ExtremeCloud**, the MLAG becomes a configuration of the **ExtremeCloud**. Thereafter, any changes to the MLAG configuration must be applied only from the **ExtremeCloud** - you cannot do MLAG configuration changes directly on the switch.

MLAG peers must meet the prerequisites. For more information, see [MLAG Limitations and Requirements](#).

To configure an MLAG:

- 1 Select **Configure > Devices > MLAGs > Add** from the menu.

- 2 Edit the fields:

Figure 102: MLAG Configuration

Name	Enter a unique name for the MLAG configuration.
Site	Select the site to which the switches are assigned from the list.
Switch	In each column, select the switches that will be peers.
ISC LAG Master Port	The inter-switch connection (ISC) master port for the MLAG, to which member ports can be assigned.
ISC LAG Member Ports	Assign the inter-switch connection (ISC) ports that will be added to the VLAN that has the MLAG master port. The master port is the main port under which the member ports function.

- 3 Select **Save**.

Configure an Individual Port

All of the details required to manage a switch, including a switch port, are viewed from the individual switch page.



Note

You can also use [Port Manager](#) to manage ports in bulk.

Port function refers to the type of device the port serves. There are four port types:

- **Access Point** - Connects an ExtremeCloud-enabled access point. This port is part of all VLANs that are defined for the switch.
- **Interswitch** - Serves as a point to point link to another switch. This port is part of all VLANs that are defined for the switch.
- **Host** - Connects to a host, such as a workstation, phone or printer.
- **Other** - Any other type of switch connection.

A Host or Other port can be customized. You can select:

- Which of the deployed VLANs the port belongs to
- PVID

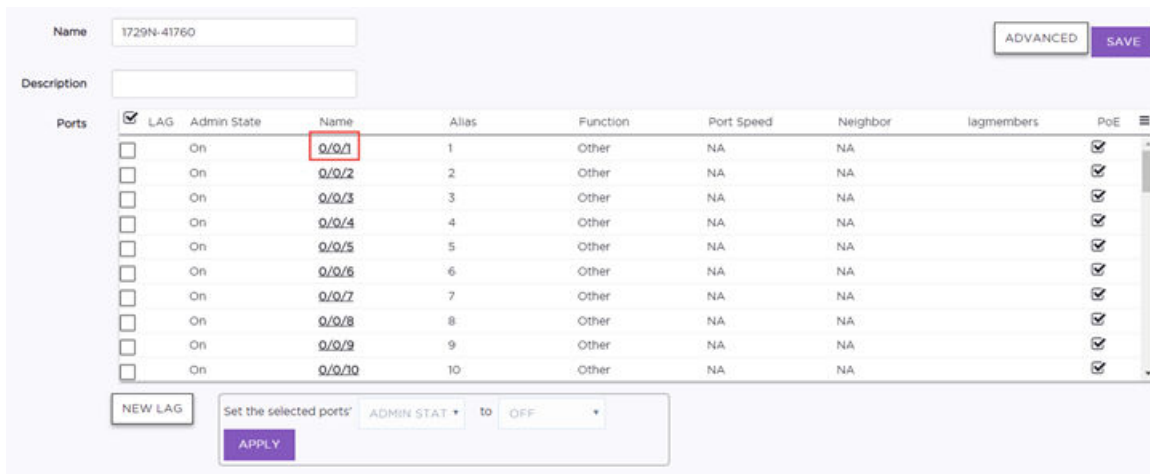
- Which VLAN egresses the port untagged

To manage and configure a switch port:

- 1 Select **Configure > Devices > Switches** from the menu.
- 2 Select a switch from the list.

The **Configure Switch** page opens.

- 3 Select a port name from the **Name** column.



The screenshot shows the 'Configure Switch' page for a switch named '1729N-41760'. The page includes a 'Description' field and a table of ports. The 'Name' column for the first port, '0/0/1', is highlighted with a red box. Below the table, there is a 'NEW LAG' button and a section to 'Set the selected ports' with a dropdown menu for 'ADMIN STAT' and a dropdown for 'to OFF', followed by an 'APPLY' button.

Ports	LAG	Admin State	Name	Alias	Function	Port Speed	Neighbor	lagmembers	PoE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	On	0/0/1	1	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/2	2	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/3	3	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/4	4	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/5	5	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/6	6	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/7	7	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/8	8	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/9	9	Other	NA	NA		<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	On	0/0/10	10	Other	NA	NA		<input checked="" type="checkbox"/>

Figure 103: Configure Switch Page

The **Configure Port** page opens.

- 4 Edit the fields.

The screenshot shows the 'Configure Port' configuration page. The fields are as follows:

- Name:** 3
- Alias:** 3
- Admin State:** ON
- Function:** OTHER
- PoE Enabled:**
- VLANs:** WING_NAT_TOPOLOGY(2500) (with a plus icon to add more)

Name	VLAN IDs	Transmit Tagged	PVID
Default	1	<input type="checkbox"/>	<input checked="" type="radio"/>

Below the table, there are fields for **VLAN Groups** (Name and VLANs) and **Categories** (with a plus icon).

Figure 104: Configure Port

- Name** Specify a port name.
- Alias** (Optional) Add a user-friendly name as an alias for the port.
- Admin State** Specify whether the port will be enabled or disabled.
- Function** Specify what the switch port will serve as a connection to **APs**, **Interswitch** (uplink), **Host** (such as a printer), **Other**, or **MLAG Interswitch**. If the switch detects an AP using LLDP, the switch will automatically provision the port for that AP. Based on the port role, ExtremeCloud configures VLAN assignments and STP settings (when enabled). You can customize the VLAN settings for **Host** or **Other**. **MLAG Interswitch** is used by MLAG peers to send health-check messages and send MLAG status checkpoint information.
- PoE** Enable or disable Power over Ethernet (PoE) as the power source.
- VLANs** If the function is set to **Host** or **Other**, you can customize the VLAN settings by assigning the port to VLANs, VLAN groups, and categories.
- VLANs** (Optional) Assign a VLAN from the drop-down list of available VLANs. Select one or more VLANs to assign or delete. A VLAN can be used in more than one VLAN group.

- VLAN Groups** (Optional) VLAN Groups are topology groups that contain one or more VLAN IDs. VLAN groups can be assigned to a port or a group of ports, and each port can have more than one VLAN group assigned to it. Each VLAN group is treated as one entity. A VLAN group can also contain VLANs that have more than one VLAN ID assigned to it.
- Categories** (Optional) Add or remove from the selected ports. You can create your own category names.
- Untagged Traffic** 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. Because 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.
- Tagged Traffic** The authentication process can indicate a specific role applicable to a user, and the policy definition can dictate how the user's traffic will be presented to the network, including the need to tag traffic to a specific VLAN.
- PVID** Specifies that the Port VLAN ID (PVID) will be the default VLAN ID assigned to untagged frames coming in to the port.
- 5 Select **Advanced** and edit the fields. The maximum speed and duplex that can be set to a set of ports is the lowest capability of any port in the set.

Note



For switches that do not support half-duplex, the copper switch ports must have the automatic negotiation disabled and full duplex enabled when connecting 10/100/1000 Mbps devices that do not automatically negotiate. If the switch attempts and fails to automatically negotiate with its partner, it will fail to link up. A non-negotiating connected device must also be manually configured for full duplex or packet loss and port errors will occur each time it detects a collision.

Advanced Port Settings ?

Port Speed AUTO ▾

Port Duplex FULL ▾

Energy Efficient Ethernet

CLOSE

Figure 105: Advanced Port Settings

- Port Speed** Set the port speed to **Auto**, **1G**, **10M**, or **100M**. **1G** is typically a small form factor pluggable (SFP) fiber port. **10M** and **100M** are copper ports. **Auto** specifies that the port will automatically negotiate the port speed.
- Port Duplex** Set the port duplex setting to **Full** or **Half**. Half duplex means that frames can only flow in one direction at a time. Full duplex allows frames to flow in both directions at the same time.
- Energy Efficient Ethernet** When enabled, this setting reduces power consumption during periods of low data activity.

- 6 Select **Save**.

CLI Mode

CLI mode is the remote command line interface (CLI) option that allows switch configuration using the command line from the **ExtremeCloud** user interface.

CLI Mode Features

In addition to providing a terminal session, the CLI features include:

- **Statistics reporting** - Statistics will continue to be reported to **ExtremeCloud**.
- **Backup and restore** - The initial backup is automatic. Administrators are responsible for creating additional backups. Up to two backups can be saved and restored.
- **Audit logs** - Audit logs are maintained for enabling and disabling CLI mode, starting and stopping a terminal session, and initiating a backup or restore request. Cloud audit logs do not track CLI configuration changes because the configuration is done on the switch. To track configuration changes, you can use a local system log server and enable cli-configuration-change logging on the switch.
- **Advanced Settings** - Advanced settings include changing back to GUI mode, rebooting, and replacement (RMA) of the switch by moving its configuration to a replacement switch.

Permissions

Full administrators, power administrators, and MSP administrators with read/write permissions can configure a switch in CLI mode.

Users with read-only permissions cannot change the configuration mode or start a CLI session on the switch, but they can view the switch in CLI mode.

Enabling CLI Mode

CLI mode is enabled on individual switches only and cannot be enabled as a bulk operation.

Enabling CLI mode disables the automatic assignment of any new configuration to the switch from GUI mode. For example, if a change is made to a site configuration, the change will not be propagated to the switches that are in CLI mode.

A switch that is put into CLI mode will continue to operate with its pre-existing configuration until a set of CLI commands are applied to it.

The best practice is to enable CLI mode only for switches that provide special services, such as routing. It is a best practice to leave outer edge switches in GUI mode.

Enabling CLI mode does not disrupt service. However, if a switch is in a red state, wait until the switch is in a green state before putting it in CLI mode so that the switch does not get out of synchronization with the cloud.

Disabling CLI Mode

Disabling CLI mode and changing back to GUI mode will disrupt service. The switch will be reset to factory settings, and then completely reconfigured based on the global settings, site-specific settings,

port types, and default settings for the switch model and site to which the switch is assigned. To minimize the impact of switching to GUI mode, you can schedule the mode change for off-peak hours.

Special Considerations

Some switch features will not work, such as stacking, with CLI mode.



Caution

Do not stack the switches. Stacking is not supported in cloud management. If you enable stacking in CLI mode, most of the switches in the stack will not be monitored. Also, the stack will not be able to identify the master, resulting in reporting on the nodes instead.

If a switch is part of an MLAG pair, you must either enable CLI mode on both switches or use GUI mode on both switches. If you enable CLI mode, the user interface shows the switches as being peers and statistics are processed accordingly, regardless of any changes you make in CLI mode.

If a controlling bridge switch is placed in CLI mode, the bridge port extenders (BPEs) are placed in CLI mode automatically. BPEs cannot be directly configured; only the controlling bridge is configurable.

Upgrades to the operating system will be sent from **ExtremeCloud** to the switch when it is in CLI mode.

More Information

- [Use CLI Mode](#) on page 157

Use CLI Mode

CLI mode lets power administrators, full administrators, and MSP administrators configure a switch using commands from the **ExtremeCloud CLI Mode** interface.



Note

Read-only administrators can view a configuration from the **CLI Mode** interface, but cannot make any changes to the configuration.

Enabling CLI mode disables the automatic assignment of configuration to the switch. The switch will continue with its existing configuration until CLI commands are applied to it. We recommend that you review the [CLI mode concepts](#) before enabling CLI mode.

To use CLI mode:

- 1 Log in to **ExtremeCloud** with either Power Administrator or Full Administrator (read/write) credentials.
- 2 Select **Configure > Devices > Switches** from the menu, and select a switch from the list.
- 3 Select **View Configuration > Advanced**.

- In the **Advanced Settings** dialog, select **Change to CLI Mode**. Read the warning, and select **Continue**. (Select **Cancel** to cancel the action.)

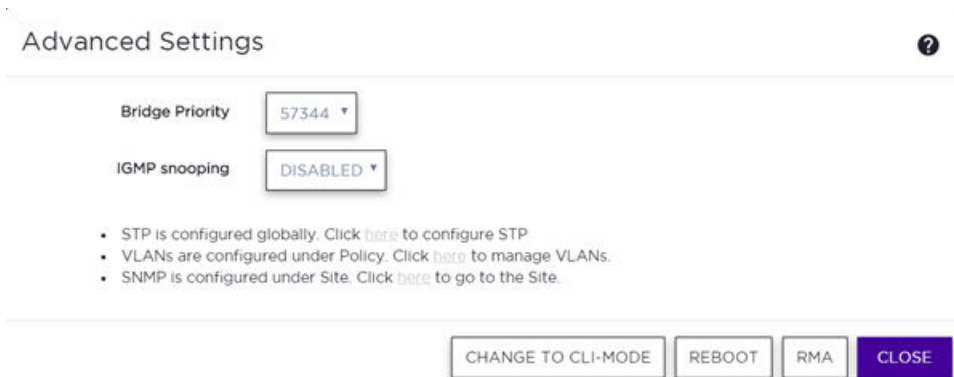


Figure 106: Advanced Settings

ExtremeCloud puts the switch in CLI mode and uploads a backup copy of the switch configuration. This process can take several minutes. Wait a few minutes after putting a switch into CLI mode before making changes through the CLI console.

- To open a terminal window, select **Activate Console**.

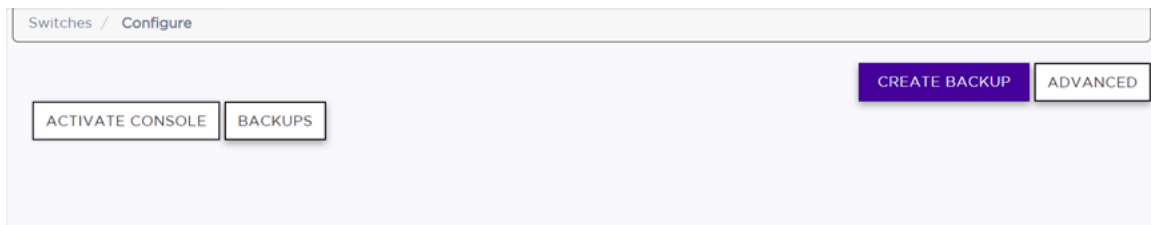


Figure 107: Activate Console Option

The terminal window opens.

- Above the terminal window, select **Click here to get login credentials** to reveal the username and randomly generated password for the default administrator. The username is always **cliadmin** on every switch, but the password will be different on every switch. The best practice is to immediately change the password to something you can remember, and keep careful track of your passwords.

Important



The randomly generated password will only be visible a few times, then will **never** be displayed again. A message displays telling you the date that the credentials will stop showing in the user interface.

Note



If you forget the password, [contact Support](#) to ask them to assign a new password to the cliadmin account. Alternatively, you can use the one-time failsafe password procedure in the GTAC knowledge base (article number [000008964](#)) to log in to the serial console, then assign a known password or create a new password.

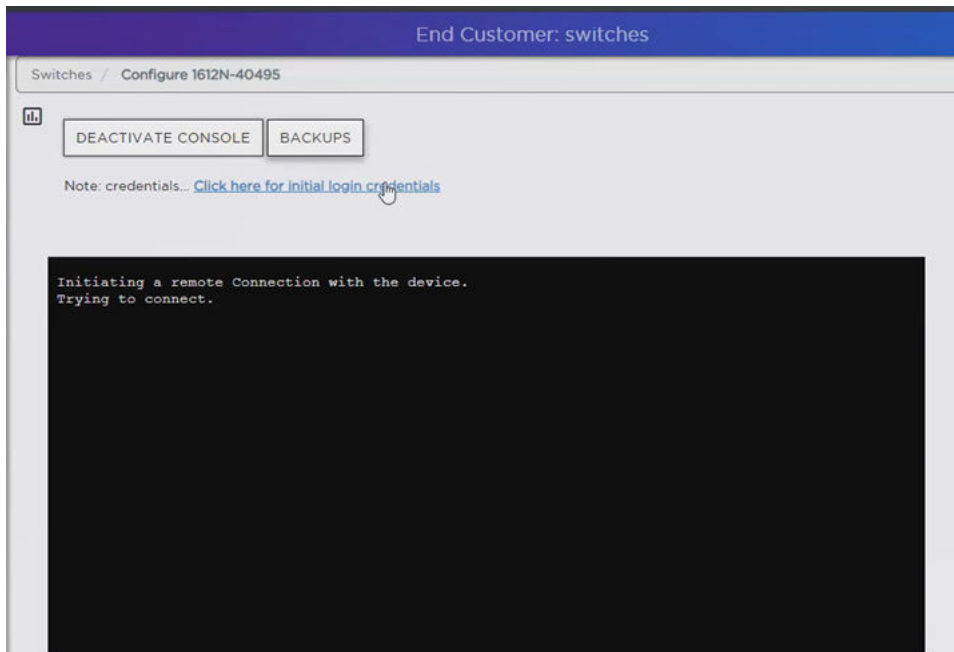


Figure 108: Active Console

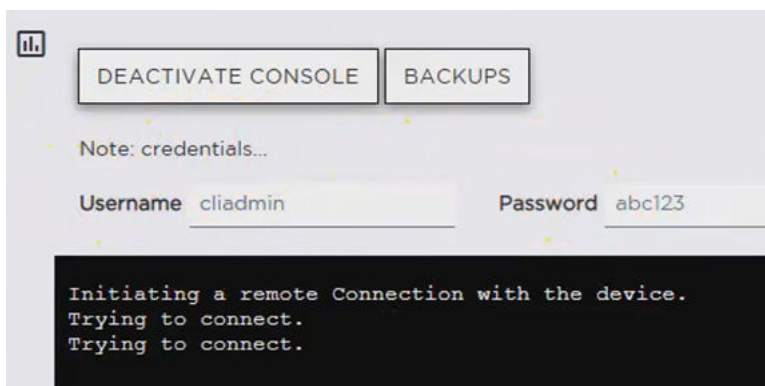


Figure 109: Login Credentials Displayed

- 7 In the terminal window, log in to start a session. When you log in as the default administrator (cliadmin), you can create additional accounts and run configuration commands. Use the terminal window to type a command, or copy and paste one command line at a time. A previous, saved script displays if the window was not cleared in the earlier session. To end the session, select **Deactivate Console**.



Caution

Do not stack the switches. Stacking is not supported in cloud management. If you enable stacking in CLI mode, most of the switches in the stack will not be monitored. Also, the stack will not be able to identify the master, resulting in reporting on the nodes instead.

- 8 To view the most recent backup, select **Backups**. You can also view previous backups, if available. A maximum of two backups are retained.

- 9 To backup the current switch configuration, select **Create Backup**. Except for the initial backup when CLI mode is enabled, all subsequent backups are initiated manually by the administrator. Backups do not disrupt service.

The backup is stored in **ExtremeCloud**.

- 10 To restore the latest backup or a previous backup, select **Restore**. Restoring a backup will disrupt service because the switch must be restarted to apply the new configuration.



Note

ExtremeCloud sends operating system (OS) upgrades to the switch. Backup configurations are expected to work with OS upgrades.

- 11 To switch back to GUI mode, reboot, or RMA the device, [use the CLI mode advanced settings](#).
- 12 Select **Save**.
Your changes are saved and applied to the switch.

Use Advanced CLI Mode Settings

In CLI mode, you can change back to GUI mode, reboot, or RMA the device using the advanced settings.

To use the CLI advanced settings:

- 1 From the **CLI Mode** page, select **Advanced**.
- 2 In the **CLI Advanced Settings** dialog, edit the fields.

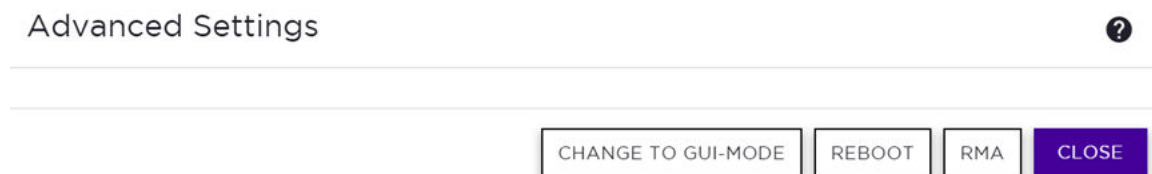


Figure 110: CLI Advanced Settings

GUI Mode Using GUI mode is optional. Changing back to GUI mode disrupts service. (The best practice is to use the **Schedule** option to put the switch into GUI mode during off-peak hours.) Changing to GUI mode also disables the CLI switch credentials if the switch is put into CLI mode again. In this case, a new random password is generated and displays in the user interface.

Reboot Restarts the switch.

RMA Select which existing switch to replace with the new switch. (The list of available switches only shows switches that have the same hardware and locally installed licenses.) The new, replacement switch is put into CLI mode. It can take an hour or more to download the configuration from the existing switch to the replacement switch.

- 3 Select **Save**.

13 Configuring Policy

Roles

Network Policy Rules

Application Policies and Application Rules

Class of Service and ToS/DSCP

Tagged and Untagged VLANs

Configure Rates

How to Configure a Captive Portal

How to Limit Bandwidth

The **Policy** section of the user interface lets administrators configure and manage roles, rules, class of service, VLANs, rates, and captive portal.

More Information

- [Configure Roles](#) on page 162
- [Configure L2, L3, and L4 Rules](#) on page 164
- [Configure L7 Application Rules](#) on page 170
- [Configure Extended Application Rules](#) on page 172
- [Configure Class of Service](#) on page 174
- [Configure Rates](#) on page 181
- [How to Limit Bandwidth](#) on page 201

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, Staff, or Guest. Often, role names will 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 (Default Unauth) role will be used while the client is not authenticated but able to access the network. The default authenticated role will be assigned to a client if it completes authentication successfully but the authentication process did not explicitly assign a role to the client.

The Default Unauth role lets you control access to sensitive information and protocols. After a wireless client authenticates, a default role is applied when:

- The RADIUS server that authenticates the user does not specify a filter ID to apply to the user's session.

- The filter ID returned by the RADIUS server does not correspond to a role defined for the group.



Note

Default roles are created on the **Networks** page.

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.

More Information

- [Configure Roles](#) on page 162
- [Configure L2, L3, and L4 Rules](#) on page 164
- [Configure L7 Application Rules](#) on page 170

Configure Roles

Roles are assigned to clients, and the assigned role follows the client as they roam around the network. The default non-authenticated role is assigned to a client automatically when it accesses the network. If MBA or WPA2 Enterprise w/ RADIUS is configured for the network, then the RADIUS server performing the authentication can assign the client to a different role that is not the default role.


Rules are one or more actions to take on a packet matching criteria. A role can contain a maximum of 64 rules. Any combination of rules are supported. Only the policy rules assigned to a client are applied to a client's traffic. If no rule is defined, the role's default action is taken. Allowed traffic can also be assigned a Class of Service. For more information, see [Matching Policy Rules Criteria](#).

To define roles that the RADIUS server can assign to clients, but which are not necessarily used as the default role for a service:

- 1 Select **Configure** > **Policy** > **Roles** from the menu.
The **Roles** list displays.
- 2 Select **Add** to create a new role. Alternatively, select a role from the list and select **Configure Role**.
The **Configure Role** page opens.
- 3 Edit the fields.

Figure 111: Configure Role Page

Name Roles are usually named for a type of user, such as Student, Doctor, Guest, or Staff. If RADIUS servers are used, the role name should match the filter ID values set up on the RADIUS servers.

Bandwidth Limit When this option is selected, a slider displays that lets you set the limit. Optionally, select  to either edit the CoS under the bandwidth limit or select a pre-defined CoS and modify it. (Using a pre-defined CoS does not require using the bandwidth slider.)

**Note**

For more information about CoS, see [Configuring Class of Service](#).

Default Action The default action is applied when the current packet does not match any of the role's rules.

Allow Allows the packet to be forwarded on the network's default VLAN.

Deny Any packet that does not match a rule in the role is dropped.

Contain to VLAN Specifies that traffic not matching any of the role's rules will be forwarded on the VLAN specified in the **VLAN IDs** field.

VLAN IDs Specify the VLAN ID. This only applies if the role's default action is **Contain to VLAN**.

**Note**

Including multiple VLANs in the VLAN ID field causes ExtremeWireless WiNG APs to load balance traffic across all of the listed VLANs. This is an advanced option and should only be enabled in special cases. APs use the lowest numbered VLAN in the list and do not load balance across the VLANs.

- 4 (Optional) To configure a Layer 2 rule, expand the **L2** section using the corresponding down arrow, expand the **L2**. Select a rule from the list to edit or select **New** to add a rule.
- 5 (Optional) To configure a Layer 3/4 rule, expand the **L3,L4** section using the corresponding down arrow. Select a rule from the list to edit or select **New** to add a rule.
- 6 (Optional) To configure a Layer 7 (application) rule, expand the **L7** section using the corresponding down arrow. Select a rule from the list to edit or select **New** to add a rule.
- 7 Select **Save** on the **Configure Role** page.

For more information about roles, see [Roles](#) on page 161.

Network Policy Rules

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.

A *network rule* defines one or more actions to take on a packet matching criteria specified by the rule (such as IP address or port number). The actions can be to deny the traffic, to allow the traffic, to contain the traffic to a specific VLAN. 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**

Application policies and application rules apply to application access and use different matching criteria.

More Information

- [Configure Roles](#) on page 162
- [Configure L2, L3, and L4 Rules](#) on page 164
- [Configure L7 Application Rules](#) on page 170

Matching Criteria for Network Rules

A policy rule consists of:

- Match criteria
- An optional access control action (allow, deny)
- An optional Class of Service assignment

Network policy rules can match on:

- Source MAC address
- Destination MAC address
- IPv4 Source IP address
- IPv4 Destination IP address
- Source Layer 4 port
- Destination Layer 4 port
- IPv4 Source socket (IP address + port)
- IPv4 Destination socket (IP address + port)
- IP type
- ICMP packet type and code
- ToS/DSCP marking
- 802.1p priority
- Ethertype
- Fully Qualified Domain Names (FQDNs) and FQDN suffixes

Policy rule access control actions can be:

- **Allow** - Forwards matching frames on the WLAN Service's default VLAN.
- **Deny** - Drops matching frames.
- **Contain to VLAN** - Forwards matching frames on the indicated VLAN.
- **None** - Specifies that the rule does not have an access control action. The matching engines essentially ignore a rule with an access control action of None.

Configure L2, L3, and L4 Rules

Customized network rules can be configured from the **Roles** page. Rules can also be configured for the default role from the **Network** page.



Note

ExtremeWireless WING APs always apply L2 rules before trying any other rules.

For information about configuring Layer 7 application rules, see [Configure L7 Application Rules](#) on page 170.

To configure network rules for Layer 2, 3, or 4:

- 1 Select **Configure > Roles** from the menu.
The **Roles** list displays.
- 2 Select **Add** to add a new role. Alternatively, select an existing role to open the **Configuration** page.
- 3 To configure a Layer 2 or Layer 3 rule, expand the corresponding arrow for the rule type you want to configure. To create a new rule, select **New**. Edit the fields in the new row that appears. The editable fields that display for a rule depend on the rule type.



Note

The rules are applied from top to bottom.

Order	Name	Action	CoS	MAC Address	MAC Address Type
1		ALLOW	NONE		ANY MAC

Figure 112: Edit and Set Order for Layer 2 Rules

- | | |
|--------------------|---|
| Name | Specify a name for the rule. |
| Action | Specify the action that the rule will take (Allow, Deny, Contain to VLAN or Redirect). A redirect rule requires a URL to redirect to. |
| CoS | Specify a class of service (None, No CoS, Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, High Priority). |
| MAC Address | Specify the destination MAC address for the selected policy rule. |
| Mask | (Layer 2/3) Works with the hexadecimal value being used 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. |
| Protocol | Specify the protocol to be used to send error messages and operational information, such as when a requested service is not available or a host cannot be reached. |
| Subnet | If left blank, the rule will use all subnets. The FQDN option allows filtering on fully qualified domain names. This can be used with the captive portal option (Cloud or Other when configuring the network service and allows the creation of a walled garden. |
| Port | Specify the port to use. |
- 4 To further edit the rule details, select . The editable fields that display for a rule depend on the rule type (Layer 2 or 3).



Note

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

Rules ?

Direction

From User DESTINATION (DEST) ▾

To User SOURCE (SRC) ▾

Layer 2 Classification

Ethertype INTERNET PROTOCOL, VERSION 4 (IPV4) ▾ 0x

MAC Address ANY MAC ▾

Priority ANY PRIORITY ▾

Action

^ ▾
Access Control ALLOW ▾

Class of Service NONE ▾
+

Figure 113: Layer 2 Rules Configuration

- From User** Select which IPv4 or IPv6 addresses in the IP header to match for traffic flowing from the client to the network. Options include: None; Source; Destination
- To User** (Advanced) Specify which IPv4 or IPv6 addresses in the IP header to match for traffic flowing from the network to the client. Options include: None; Source; Destination
- Ethertype** (Layer 2) The rule filters based on any Ethertype or a specified Ethertype (IPv4, IPv6, ARP).
- Priority** Specify the priority. Priority 1 is the highest priority.

Rules

Direction

From User DESTINATION (DEST) ▾

To User SOURCE (SRC) ▾

Layer 3 Classification

IP Subnet USER DEFINED ▾

Port ANY PORT ▾

Protocol ANY PROTOCOL ▾

ToS/DSCP 0x (DSCP: 0x) CONFIGURE **Mask:** ▾

Action

Access Control ALLOW ▾

Class of Service NONE ▾ +

Figure 114: Layer 3 Rules Configuration

- IP Subnet** (Layer 3/4) Enter a valid IP subnet. To filter on a fully qualified domain name (FQDN), select FQDN from the drop-down list and enter the FQDN name in the text box. Filters are supported for full names (www.companyname.com) or partial names (companyname.com).
- Port** (Layer 3/4) Specify the port that will be used.
- Protocol** (Layer 3/4) Specify the protocol that will be used.
- ToS/DSCP** (Layer 3/4) Enter a hexadecimal value in the **0x (DSCP:)** field, or select **Configure** to open the ToS/DSCP dialog.
- Mask** Works with the hexadecimal value being used 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.

- 5 Set the **Access Control** and the **Class of Service**.

The screenshot shows a configuration interface for an 'Action'. It features two dropdown menus. The first, labeled 'Access Control', is set to 'ALLOW'. The second, labeled 'Class of Service', is set to 'NONE'. To the right of the 'Class of Service' dropdown is a plus sign icon in a square button.

Figure 115:

Access Control	Specify the access control.
None	No role is defined.
Allow	Packets will be contained to the role's default action VLAN.
Deny	Any packet not matching a rule in the policy is dropped.
Contain to VLAN	Specifies that traffic not matching any of the role's rules will be forwarded on the VLAN specified in the Contain to VLAN ID field.
Redirect	Indicates redirect action and requires a URL to redirect to. Rules-based redirection occurs upon a deny action when Redirect is enabled and a rule is defined for redirection.
Class of Service	Displays when you select Contain to VLAN . Assign a class of service.

- 6 Select **Close**.

You return to the **Configure Role** page.

- 7 Select **Save**.

All rule types are applied to the policy in top to bottom order. The policy is installed on the enforced APs.

For more information about network rules, see [Network Policy Rules](#) on page 163 and [Matching Criteria for Network Rules](#) on page 164. For information about Layer 7 application rules, see [Application Policies and Application Rules](#) on page 168.

Application Policies and Application Rules

- [Overview](#) on page 168
- [Rules](#) on page 169
- [Actions and Limitations](#) on page 169
- [More Information](#) on page 169

Overview

Application control policies (application policies) let you define rules that dictate how each traffic type is managed on your network. An application policy contains at least one application (Layer 7) rule.

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 contents
- Blocking or limiting peer-to-peer protocols to preserve bandwidth and flows for other applications
- Limiting bandwidth usage by non-business related traffics, such as YouTube

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



Note

Application policies are supported by ExtremeCloud-enabled APs only, not switches.

Rules

Application policies consist of rules with match criteria, coupled with one or more actions to take when a packet matches the rule's criteria. The match criteria for an application usually is just the name of the application. Since cloud-enabled APs recognize thousands of applications, the ExtremeCloud 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 'any' as the specific application.

Custom application rules are rules that you create to recognize (match) applications that are not in the pre-defined set of application matches provided by ExtremeCloud. 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.

More Information

- [Configure Roles](#) on page 162
- [Configure L2, L3, and L4 Rules](#) on page 164
- [Application Policies and Application Rules](#) on page 168
- [Whitelist Applications](#) on page 173

Configure 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 any number of application rules in one role.



Note

ExtremeWireless WiNG APs always apply L2 rules before trying any other rules.

To configure application rules:

- 1 Select **Configure > Roles** from the menu.
- 2 Select **Add** to add a new role. Alternatively, select an existing role to open the **Configuration** page.
- 3 Expand the **L7 Rules** section. To create a new rule, select **New**. Edit the fields in the new row that appears. Alternatively, select an existing row to edit.



Note

The rules are applied from top to bottom.

Order	Name	Action	COS	Search	Application Group	Application Name
1	Videos	ALLOW	NONE	Search Appl	EDUCATION	

Figure 116: Edit and Set Order for Layer 7 Rules

Name	Specify a name for the rule.
Action	Specify the action that the rule will take (Allow, Deny, Contain to VLAN or Redirect). A redirect rule requires a URL to redirect to.
CoS	Specify a class of service (None, No CoS, Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, High Priority).
Search	Lets you search on an application group name or on an individual application name.
Group	Specify the application group to which the application belongs. The groups are pre-defined and cannot be customized.
Application Name	Enter a unique name for the custom application.

- 4 To further edit the rule details, select . Edit the fields.

Direction


From User

To User

Application

Search

Group

Application 

Note : Applications with (+) applies to IDENTIFI family and (-) applies to WING family (+-) applies to both the families

Action

Access Control


Class of Service 


Figure 117: Application Rules Configuration

- Search** Lets you search on an application group name or on an individual application name.
- Group** Specify the application group to which the application belongs. The groups are pre-defined and cannot be customized.
- Application** Specify the application name from the drop-down list. You can create a new rule anywhere in a policy, and create any number of application rules in a policy. For example, you can create a Web Application policy to limit the rule to web applications only.



Note

The  button lets you [create an extended \(global\) application](#) from the selected application.

- 5 Set the access control from the drop-down list and Class of Service. Select  to [add a Class of Service](#).
- 6 Select **Close** > **Save**.
- All rule types are applied to the policy in top-to-bottom order. The policy is installed on the enforced APs.

If needed, you can create a policy to [whitelist one or more applications](#). For more information about application rules, see [Application Policies and Application Rules](#) on page 168.

Configure Extended Application Rules

Extended applications are customized rules that are created from application rules. This rule is separate from a policy rule, but it can be referenced by a policy rule. The extended signatures are global, so an extended signature created on one rule is available to be used in other policies.

This rule type is optional.



An administrator can create up to 128 extended applications. These rules can be modified.



Note

The rule is not shared between customers in an MSP environment.

To configure extended application rules:

- 1 Select **Configure > Roles** from the menu.
The **Roles** list displays.
- 2 Select **Add** to add a new role. Alternatively, select an existing role to open the **Configuration** page.
- 3 For application policy rules, expand the **L7 Rules** section.
- 4 Select **New** to add a new rule, then select  next to the new rule in the **Rules** list.
The **Application Rules** dialog opens.
- 5 Next to the **Application** field, select .
- 6 Select **Create New Application**.

Group	Application Name	Pattern

Figure 118: Custom Applications Dialog

The Application Settings dialog opens.

- 7 Edit the fields.

The screenshot shows a dialog box titled "Application Settings" with a help icon (question mark) in the top right corner. The dialog contains three input fields: "Group" with a search box containing the text "Search Groups", "Name" with an empty text box, and "Pattern" with an empty text box. At the bottom right of the dialog are two buttons: "CANCEL" and "OK".

Figure 119: Application Settings Dialog

Group Specify the application group to which the application belongs. The groups are pre-defined and cannot be customized.

Application Name Enter a unique name for the custom application.

Pattern Enter all or part of a fully qualified domain name (FQDN). The rule will match if the text that you enter appears anywhere in the host header of HTTP traffic. **Example:** The pattern **companyname** will match 'www.companyname.com', 'companyname.com' and 'www.company-name.com'. The match is case sensitive, so the pattern will *not* match 'Companyname.com'.

- 8 Select **OK**.
- 9 Select **Close** in the **Rules** dialog, and then select **Save**.

The extended application rule is applied to the policy, and is made available to other policies.

Whitelist Applications

You can create a policy to block everything except a single application or small group of applications (or web sites).

To whitelist one or more applications:

- 1 Select **Configure > Roles** from the menu.
- 2 Select **Add** to add a new role. Alternatively, select an existing role to open the **Configuration** page.
- 3 Create a Deny policy to block everything. This policy can be assigned to a public user SSID.
- 4 [Add an extended application policy](#) to allow a single web site. From the **Configure Role** page, select **New Application Policy**.

A new row is added to the **Rules** list.

- 5 Select  and configure the application rule.

- 6 Next to the **Application** field, select .

The **Custom Applications** dialog opens.

- 7 Select **Create New Application** and configure the fields in the **Application Setting** dialog that opens. For example, to allow access to `www.companyname.com`, enter Web Applications as the group, Company Name as the name, and `www.companyname.com` as the pattern.

Group	Specify the application group to which the application belongs. The groups are pre-defined and cannot be customized.
Application Name	Enter a unique name for the custom application.
Pattern	Enter all or part of a fully qualified domain name (FQDN). The rule will match if the text that you enter appears anywhere in the host header of HTTP traffic. Example: The pattern companyname will match 'www.companyname.com', 'companyname.com' and 'www.company-name.com'. The match is case sensitive, so the pattern will <i>not</i> match 'Companyname.com'.

- 8 Repeat step 4-7 as needed to add additional individual web sites that each allow one web site. For example, if you want to allow five web sites, make an extended application rule for each web site, for a total of 5 extended application rules.

Class of Service and ToS/DSCP

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.

More Information

- [Configure Class of Service](#) on page 174

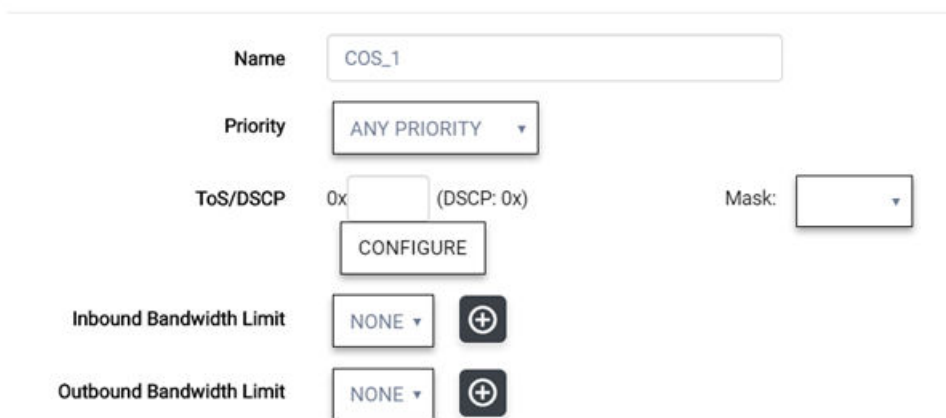
Configure Class of Service

The set of rules included in a role, along with any access or Class of Service (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.

To configure CoS:

- 1 Select **Configure** > **Policy** > **Class of Service** from the menu.
- 2 Select **Add**, or select an existing Class of Service from the list.
The **Class of Service Configuration** page opens.
- 3 Edit the fields.

COS_1



The screenshot shows the configuration page for a Class of Service named 'COS_1'. The fields are as follows:

- Name:** COS_1
- Priority:** ANY PRIORITY (dropdown menu)
- ToS/DSCP:** 0x [] (DSCP: 0x) with a CONFIGURE button below it.
- Mask:** [] (dropdown menu)
- Inbound Bandwidth Limit:** NONE (dropdown menu) with a plus icon button.
- Outbound Bandwidth Limit:** NONE (dropdown menu) with a plus icon button.

Figure 120: Class of Service Configuration

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.


- 5 (Optional) In the **ToS/DSCP** dialog, select either **Type of Service (ToS)** or **Diffserv Codepoint (DSCP)**. Set the related options, and select **OK**.

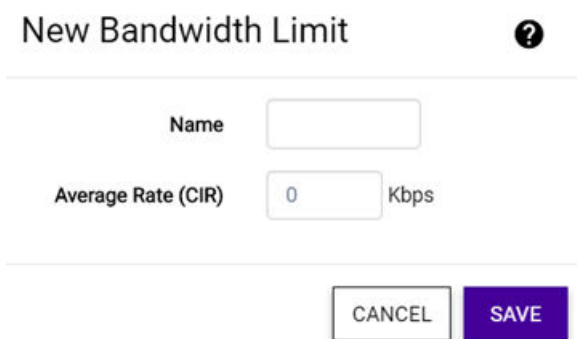
Figure 121: ToS/DSCP Configuration


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.
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.

- 6 In the **CoS** dialog, 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.

- 7 Select the inbound and outbound bandwidth limits from the drop-down lists. If needed, select  to configure new bandwidth limits.



New Bandwidth Limit 

Name

Average Rate (CIR) Kbps

Figure 122: New Bandwidth Limits Dialog

Inbound Bandwidth Limit	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, role, or WLAN. 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 Bandwidth Limit	Outbound traffic is sent from the network towards the client. Maximum Number of Limiters per Group: 8 outbound

- 8 Select **Save**.

Tagged and Untagged 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.

It is not necessary to include a VLAN tag in a packet that is being transmitted over a VLAN. A packet transmitted without a VLAN tag is said to be untagged. Since there is no way to identify the VLAN to which an untagged packet belongs, there can be only one untagged VLAN on a VLAN trunk.

It is common practice to place all AP management traffic on an untagged VLAN and place user traffic on tagged VLANs. ExtremeCloud preconfigures switches with a single untagged VLAN that is used for managing access points and the switches themselves.

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

ExtremeCloud 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.

All administrator-created VLANs in ExtremeCloud 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.

More Information

- [VLAN Support for Switches](#) on page 178
- [Configure VLANs](#) on page 179
- [Configure VLAN Groups](#) on page 181

VLAN Support for Switches

- [Tagged and Untagged VLANs](#) on page 177
- [VLAN Groups](#) on page 178
- [Port Manager Overview](#) on page 202

VLANs

ExtremeCloud switches implement support for 802.1q static VLANs. Protocol-based VLANs and port-based VLANs are not supported.

VLANs are configured under policy. A default VLAN is assigned, which maps to the default VLAN (VLAN 1) on EXOS switches. This default VLAN is pre-defined and cannot be deleted. It is deployed to every switch and AP. You can edit the multicast filters for APs only. The default VLAN is the only VLAN that can be defined as untagged.

VLANs are part of role and network configuration. VLANs are deployed to all devices in a site if any of the members of the site serve a network or role that uses the VLAN.

A switch's AP port is configured with all of the VLANs that the AP could transmit on.

An Uplink port gets all of the VLANs that are configured on a switch. The VLAN transmission can be [tagged or untagged](#).

Host ports and Other ports can have VLANs assigned directly from the list of VLANs that are applied to the group through the policy attachment. Host and other ports can also be configured to select which VLAN egresses as untagged. For example, a host can be directly connected to a switch and the host belongs on a VLAN that is not the default VLAN. You can remove the default VLAN from the port and assign a different VLAN that the host needs to egress untagged and make it the PVID.

VLAN Groups

VLAN Groups are topology groups that contain one or more VLAN IDs. VLAN groups can be assigned to a port or a group of ports, and each port can have more than one VLAN group can be assigned to it.

A topology can be used in more than one VLAN group.

Each topology group is treated as one entity. A topology group can also contain topologies that have more than one VLAN ID assigned to it.

VLAN groups can be assigned to individual switch ports or to switch ports at a site. When assigning a VLAN group to multiple ports, consider [using the Port Manager](#) to configure the ports in bulk (as a virtual stack).

Port Manager

Ports can be assigned to multiple switches at once, regardless of their location, using the [Port Manager feature](#). This feature is similar to switch stacking. Port Manager also lets you assign VLAN IDs and VLAN groups.

More Information

- [Tagged and Untagged VLANs](#) on page 177
- [Configure VLANs](#) on page 179
- [Configure VLAN Groups](#) on page 181
- [Port Manager Overview](#) on page 202
- [Use Port Manager](#) on page 203

Configure VLANs

A VLAN defines how the user traffic is presented through the network interface. The AP bridges all traffic between wireless clients and the VLANs to which it is exposed.

To configure VLANs:

- 1 Select **Configure > Policy > VLANS**.
- 2 Edit the fields.

The screenshot shows a configuration form for a VLAN. The 'Name' field is filled with 'vlan_1'. The 'VLAN IDs' field is empty and has a red border around it. There is a 'SAVE' button in the top right corner and an 'ADVANCED' button in the bottom left corner. Below the fields, there is a note: 'Note : Including multiple VLANs in the VLAN IDs field will cause WING APs to load balance traffic across all the listed VLANs. This is an advanced option and should only be enabled in special cases. Identifi APs will use the lowest numbered VLAN in the list and will not load balance across the VLANs'.

Figure 123: VLAN Configuration

VLAN IDs Specify the VLAN ID. This only applies if the role's default action is **Contain to VLAN**.



Note

Including multiple VLANs in the VLAN ID field causes ExtremeWireless WING APs to load balance traffic across all of the listed VLANs. This is an advanced option and should only be enabled in special cases. APs use the lowest numbered VLAN in the list and do not load balance across the VLANs.

- 3 (Optional) Select **Advanced**. In the **Advanced Settings** dialog, edit the fields, and then select **Close**.

Advanced Settings ?

Multicast bridging

Multicast Rules ADD NEW RULE ADD PRE-DEFINED RULE

Order	IP	CIDR	Wireless Replication	Group
1	192.0.2.3	32	<input checked="" type="checkbox"/>	mDNS/Bonjour
2	192.0.2.7	128	<input checked="" type="checkbox"/>	mDNSv6/Bonjour
3	192.0.2.4	32	<input checked="" type="checkbox"/>	SSDP (Dial, uPnP)
4	192.0.2.9	128	<input checked="" type="checkbox"/>	SSDP (IPv6)

IP Subnet IP Subnet CIDR

CLOSE

Figure 124: VLAN Advanced Settings

Multicast bridging

Select this option to enable forwarding of multicast traffic 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.

Add New Rule / Add Pre-defined Rule

Add one or more multicast rules if you enabled **Multicast Bridging**. A multicast rule permits any traffic that matches the rule.

Note

A multicast rule is defined as:



- The multicast IP address to which traffic is sent.
- A mask that allows a range of multicast addresses to be matched by a single rule.
- Whether to forward multicast traffic matching the rule that was received from a wireless user back to other wireless users.

IP

Enter the multicast IP address to which the traffic is sent.

CIDR

Classless Inter-Domain Routing (CIDR) is used along with the IP address to find the IP address range. The CIDR value indicates the routing prefix length (number of bits) of the IP address. When you add a predefined rule, the CIDR value is populated automatically by the multicast group you select for the pre-defined rule. Otherwise, the CIDR value is user defined.

- Wireless Replication** Select this option if you want to enable the wireless multicast replication for this group. Wireless Replication filters multicast traffic that is being sent back to the wireless AP channel or wired network.
- IP Subnet** Enter a valid IP subnet when using a captive portal.

- 4 Select **Close** > **Save**.

Configure VLAN Groups

VLAN groups are topology groups that contain one or more VLAN IDs. VLAN groups can be assigned to a port or a group of ports.

To create a VLAN group:

- 1 Select **Configure** > **Policy** > **VLAN Groups**.
The **VLAN Groups** page opens.
- 2 Select **Add** or select an existing VLAN group from the list to edit.
The **Create/Edit VLAN Group** page opens.

Name	VLAN IDs
WING_NAT_topology	2500

Figure 125: Create/Edit VLAN Group

- 3 Edit the fields:

Name Enter or change a name for the VLAN group.

VLANs From the drop-down list, select a VLAN ID to include in the group and select . Repeat this step for each VLAN ID that you want to include.



Note

To remove a VLAN ID from the list, hover over the VLAN name to display the delete (X) button. Select **X** to delete the VLAN ID from the VLAN group.

- 4 Select **Save**.
Your changes are saved.

You can either assign the VLAN group to an [individual switch port](#), [assign it to switches at a site](#), or [assign it to a group of switch ports using the Port Manager](#).

Configure Rates

You can set a data transfer rate for a policy.

To configure rates:

- 1 Select **Configure** > **Policy** > **Rates** from the menu.
- 2 Select **Add** or select an existing rate from the list.
- 3 Edit the fields.

Name

Average Rate (CIR) Kbps

Figure 126: Rate Configuration

Name Enter a name for the rate.

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**.

How to Configure a Captive Portal

ExtremeCloud offers the ability to configure a built-in captive portal splash screen. Alternatively, you can use an external captive portal (ECP), which redirects to a third-party server for authentication.

To use the built-in captive portal feature, you must:

- 1 [Configure a custom splash screen and assign it to a site.](#)
- 2 (Optional) [Configure an SMS gateway.](#)
- 3 [Configure captive portal preferences.](#)
- 4 (Optional) [Upload multiple preconfigured user accounts.](#)
- 5 (Optional) [Configure guest user accounts.](#)
- 6 [Enable the use of captive portal authentication on a network.](#)
- 7 [Assign the network to the site that has the built-in captive portal assigned to it.](#)

To use an ECP (third-party server), you must:

- 1 Enable the use of captive portal authentication on a network and select Other as the Portal Name.
- 2 Define a policy that:
 - Allows access to the ECP.
 - Allows DHCP.
 - Allows DNS Server.
 - Allows the IP address range of the default VLAN.
 - [Redirects at least some HTTP traffic to the ECP.](#)

When captive portal is enabled, cloud-enabled APs intercept the HTTP and HTTPS traffic of unauthenticated users and redirects them to the captive portal splash screen. The captive portal can then authenticate the user. (Authentication can be as simple as asking the user to select a button to accept any terms and conditions for using the network or it can ask the user for credentials.) If the user passes the captive portal criteria, the captive portal tells the cloud-enabled AP to allow the user onto

the network. The captive portal can also assign the user to one of the access control policies that is configured on the AP.

The captive portal feature is firewall friendly. All interactions with the captive portal take place through port 443 or port 80, which are routinely allowed to egress firewalls. This product also supports captive portals that are on the same side of the firewall as the AP.

The DHCP IPv4 address pool used by unauthenticated clients must be large enough to provide additional IP addresses to all APs configured with captive portal. This is because each AP creates a virtual interface on each non-authenticated policy VLAN and assigns an IP address to it from the pool.

You can create a walled garden with either captive portal option.

More Information:

- [Configure General System Settings](#) on page 224
- [Create a Walled Garden](#) on page 200

Configure a Custom Splash Screen

Use a captive portal to provide Internet access to guest users.

To configure a new splash screen:

- 1 From the left menu, select **Configure > Policy > Captive Portal**.



Figure 127: Captive Portal Configuration - Templates Tab

The **Templates** tab opens. The **Templates** tab displays three section (Splash Pages, Templates, Upload Logo) that can be expanded by selecting the corresponding arrow to the far right of each heading.

- 2 Expand the **Templates** section.

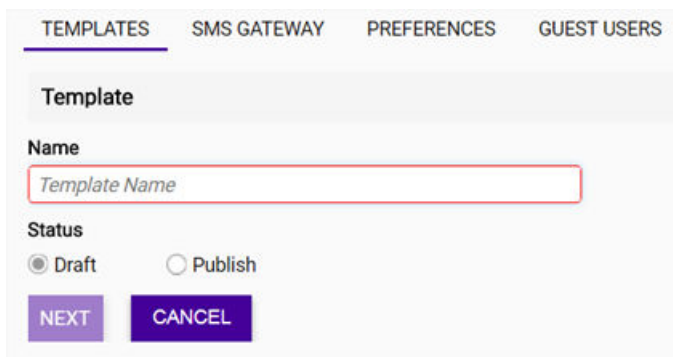
Note



Alternatively, you can duplicate and edit one of the default templates from **Splash Pages > Select Template > Default Templates**. Default, non-editable templates are provided to serve as an example when you customize your splash screens. To duplicate a default

template, select .

- To create a new splash template, select **Add**.



The screenshot shows a web interface for adding a new splash template. At the top, there are four tabs: 'TEMPLATES', 'SMS GATEWAY', 'PREFERENCES', and 'GUEST USERS'. The 'TEMPLATES' tab is selected. Below the tabs, there is a 'Template' section. It contains a 'Name' field with the placeholder text 'Template Name'. Below the name field is a 'Status' section with two radio buttons: 'Draft' (which is selected) and 'Publish'. At the bottom of the form are two buttons: 'NEXT' and 'CANCEL'.

Figure 128: Add New Splash Template

- Enter a name for the template. When you are editing a new template, you can keep the status in **Draft** mode until you preview it and determine that it is finalized. However, published templates are still editable.



Note

Only published templates can be assigned to a site. Templates that are in **Draft** mode are not made available on the list and cannot be associated with a site.

- Select **Next**.
The **Splash** and **Success** tabs appear.

- 6 On the **Splash** tab, click **Select Theme** (on the right side of the page). Do one or both of the following tasks:
- Expand the **Themes** section. Drag and drop a theme into the **Splash** pane.
 - Expand the **Modules** section. Drag and drop a module into the **Splash** pane.

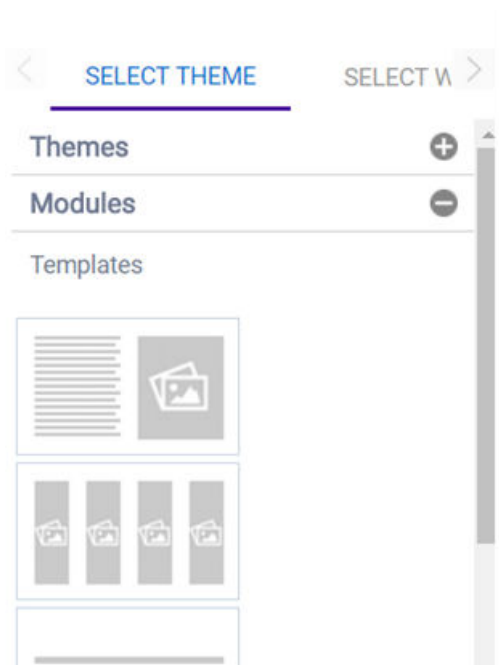


Figure 129: Select a Theme or Module

Depending on the theme selected, the **Splash** pane is divided into sections. The height of these sections can be adjusted by dragging the bottom margins.

- 7 (Optional) To change the background color, select . Use the built-in color palette to select the background color of the theme or widget that you selected.

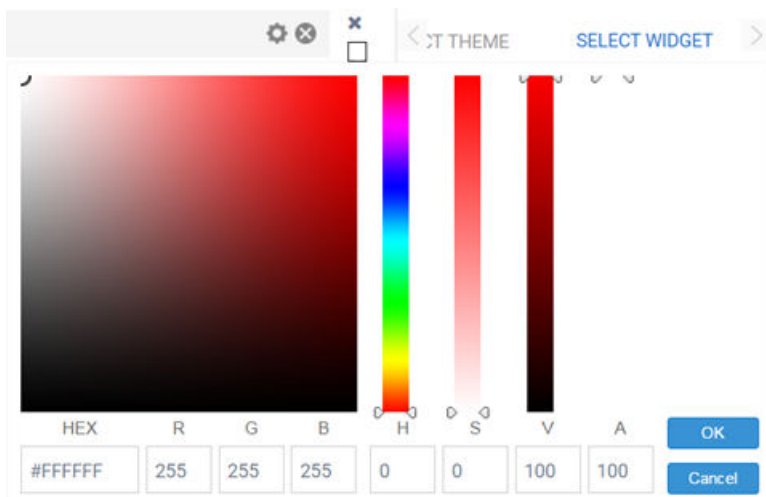


Figure 130:

- 8 Select **Page Settings**. In the **Page Setting** dialog, edit the fields. You can either upload a background image or select a background color for the remainder of the web page that lies *outside* of the **Theme** or **Widget** pane that you selected.

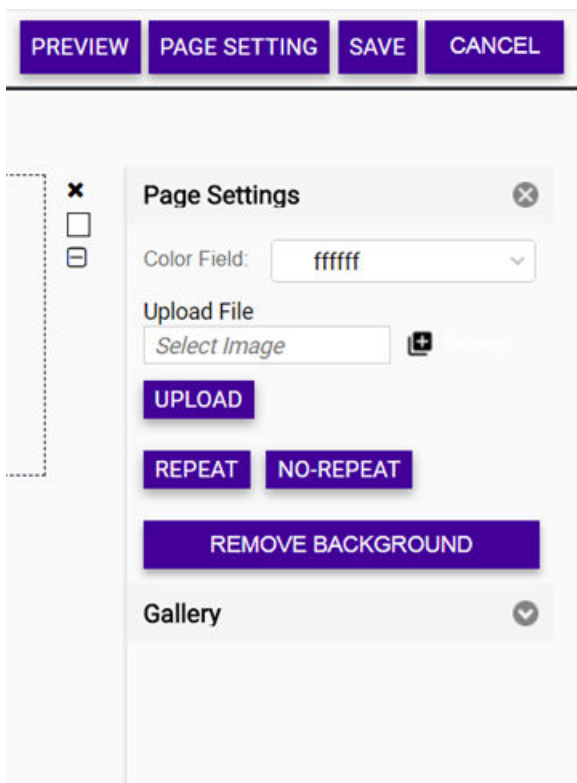



Figure 131:

Color Field Use the built-in color palette to select the background color of the splash template. This background color can be viewed in the **Preview** mode.

Upload File

Uploads and inserts a new background image. Select , and select the file on your local system. Select **Upload File**. A thumbnail of the uploaded image is also added to the **Gallery** section. Multiple images can be uploaded, however, only one image can be used as a background image at a time.



Note

If the image is small and does not cover the entire page, select **Repeat** to repeat the image as multiple tiles in the background. Select **No-Repeat** to prevent the image from displaying as tiles.

- 9 Close the **Page Settings** dialog. From the **Select Widgets** tab, drag and drop a widget to each section of the theme that you selected. Each section can contain only one widget.

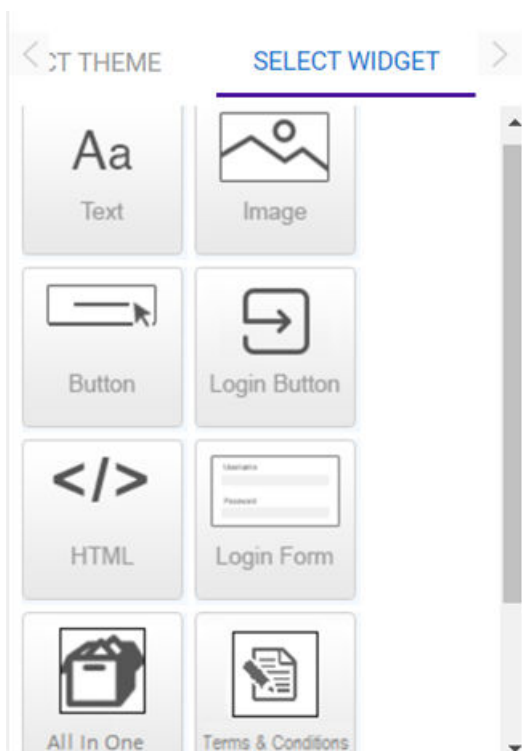





Figure 132: Widget Options

- 10 To edit the text and images in the widgets, select  to the right of a widget bar. (Edit each widget individually.) The widget editor opens. Text fonts, styles, colors, and hyperlinks can be managed using the widget toolbar. You can add an image from your local drive using **Upload File** or drag and drop an image from the **Gallery** pane. After inserting the image, customize the image placement and size using the **Alignment**, **Width**, and **Height** controls.
- 11 (Optional) To customize an **HTML** widget, select  to the right of a widget bar. The **HTML** widget lets you design your web page from scratch, without using any of the system-provided templates or widgets.
- The HTML Editor opens.

12

(Optional) To customize the **Login Button** widget, select  to the right of a widget bar. The **Login Button** widget creates a button that directs the user to a predefined URL. You can edit the URL, button label, font, color, size, alignment, and background color.

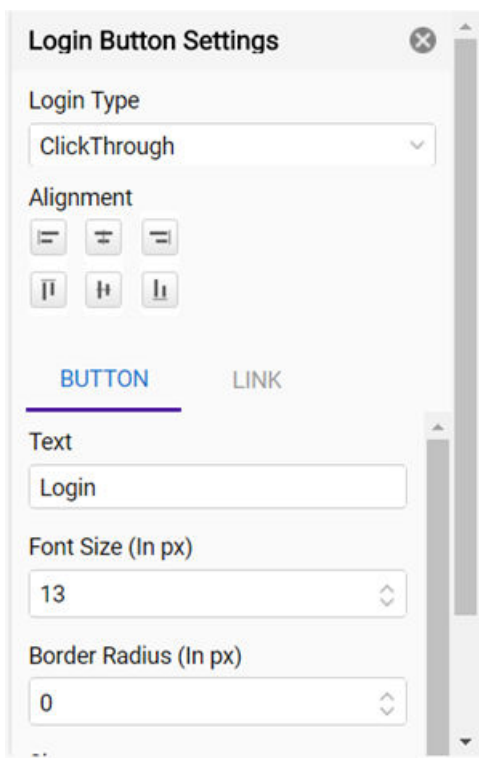


Figure 133: Login Button Settings

- 13 Select **Preview** and review your design. Use the device orientation icons at the bottom of the screen to preview the splash page as seen on different devices and orientation. The following viewing options are available for:

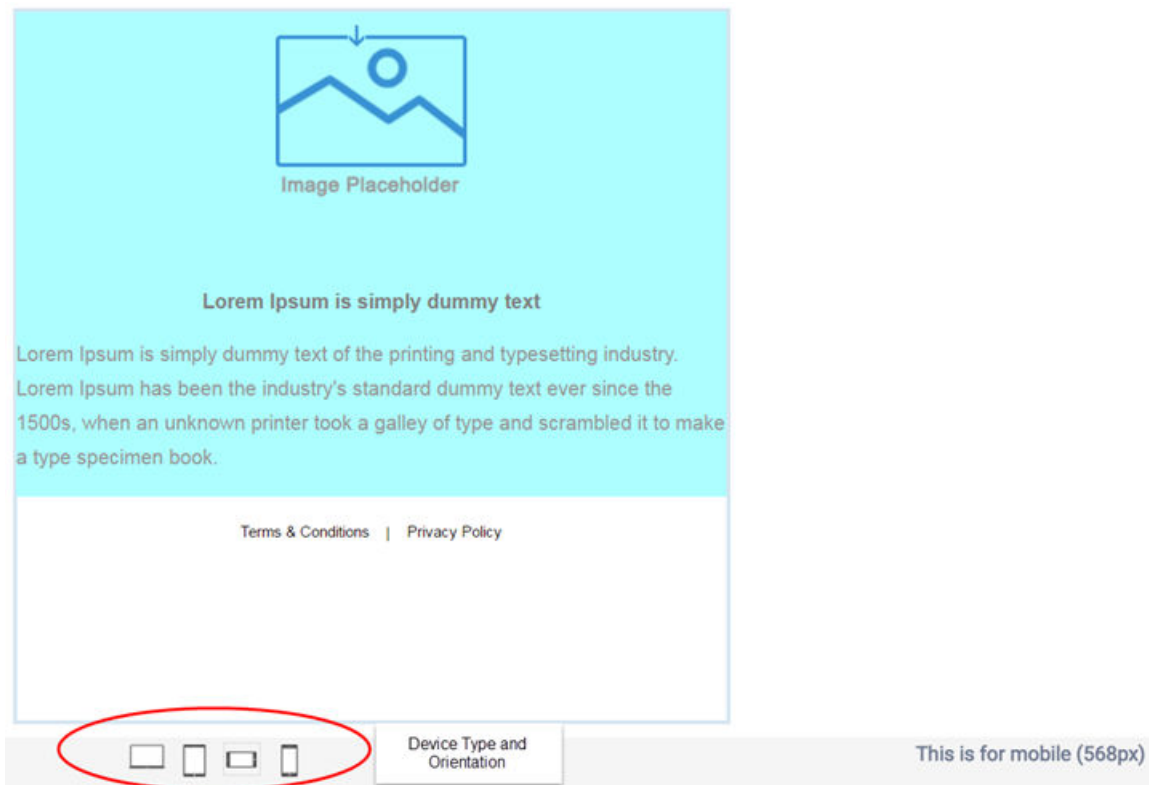


Figure 134: Device Type and Orientation Settings

- Large screen devices like laptops (960 px wide)
 - Tablets and other wide screen devices (768 px wide)
 - Mobile devices with landscape orientation (568 px wide)
 - Mobile devices with portrait orientation (320 px wide)
- 14 Close the **Preview** page and make additional edits in the **Splash** pane if needed. Select **Save**.
- 15 Repeat steps 6 - 14 to create a template for the **Success** tab.
- 16 Open the **Upload Logo** pane. Select **Upload Tenant Logo** and select an image from your local system.

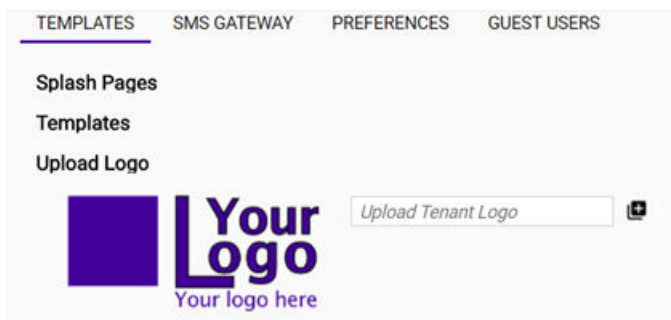


Figure 135: Upload Logo

- 17 Open the **Templates** pane. In the **Templates** menu, select the new template and select the **Status** drop-down list to put it in **Published** mode.
- 18 Expand the **Splash Pages** pane, and select **Add**. Alternatively, select an existing splash screen to edit from the list and select the pencil icon.
The **Splash Pages** page opens.
- 19 Enter a name for the splash screen and select a site from the drop-down list. (Only sites that are not assigned to a splash screen are available.) From the **Select Template** pane, select the new template. Select **Save**.

Figure 136: Configuring New Splash Page

The splash page is created and the template is assigned to the site.

Next, [configure an SMS gateway](#).

Configure an SMS Gateway

This procedure is optional.

Short Message Service (SMS) is used to send a registration code to guest users registering and agreeing to receive a one time passcode (OTP). OTP is only sent to the device used for accessing the captive portal. ExtremeCloud sends the OTP to the device and the user uses this OTP to authenticate.

Third-party SMS gateway service providers are used to provide the SMS OTP services. You must register captive portals with these third-party service providers before using OTP-based device registration.

To configure an SMS gateway:

- 1 From the left menu, select **Configure > Policy > Captive Portal**. Select the **SMS Gateway** tab.
- 2 Select **Add**. Alternatively, select an existing gateway from the list to edit.

- 3 Edit the fields:

Figure 137: SMS Gateway Tab

Name	Enter a unique name for the SMS gateway configuration.
Gateway Type	Select an SMS gateway provider from the drop-down list that will provide the SMS one time passcode (OTP) services to guest users.
Status	Specify the gateway that will be active. Only one SMS gateway can be set to Active at any time. OTPs are only sent through an active SMS gateway.
Account Details	Provide the configuration information from the third-party SMS gateway service provider. Each service provider has a different registration process for their service. The fields in this area change according to the information required by the SMS gateway service provider selected in the Gateway Type field.



Note

Select the **How to get the API details for My <SMS Gateway Service Provider> Account?** link to access the selected SMS Gateway service provider's website and obtain the required configuration information.

- 4 Select **Verify**.
The **Enter Your Number** dialog opens.
- 5 Enter a valid phone number and select **Verify**.
If configured properly, and depending on the service provider, you either receive a test SMS OTP from the service provider or a message displays about the validity of the supplied credentials.
- 6 Select **Save**.

Next, [configure the captive portal preferences](#).

Configure Captive Portal Preferences

You can configure captive portal preferences, such as the content to display for the Terms and Conditions, and to globally configure application IDs and application secrets used for authenticating with social media applications.



Note

The **Terms and Conditions** link displays on the **Splash** and **Success** panes.

To configure captive portal preferences:

- 1 From the left menu, select **Configure > Policy > Captive Portal**. Select the **Preferences** tab.
The **Terms and Conditions** section opens by default.
- 2 Edit the fields.

Figure 138: Preferences Tab

- | | |
|--------------------------------------|---|
| Custom | Enables a custom Terms and Conditions message that displays when a user logs in to the captive portal. HTML terms are editable and can be formatted. |
| URL | Enables an external URL that displays a Privacy Policy when a user logs in to the captive portal. |
| Copy and paste your text here | Enter the terms and conditions that you want to display when a user selects the Terms and Conditions link. A default Terms and Conditions message is displayed. Change the content and edit the formatting to meet your requirements. HTML terms are editable and can be formatted using the standard editing tools, such as Bold, Underline, Font Color, Highlighting, Text Placement, Bulleted List, and so on. |
| External URL | This field displays only when URL is selected. Enter the complete path to the external web page that contains the privacy policy that displays when a user logs in to the captive portal. |
- 3 Select **Save**.
 - 4 From the right of the **Privacy Policy** option, select the arrow to expand the section. Edit the fields.

Custom	Enables a custom Terms and Conditions message that displays when a user logs in to the captive portal. HTML terms are editable and can be formatted.
URL	Enables an external URL that displays a Privacy Policy when a user logs in to the captive portal.

Copy and paste your text here Enter the terms and conditions that you want to display when a user selects the Terms and Conditions link. A default Terms and Conditions message is displayed. Change the content and edit the formatting to meet your requirements. HTML terms are editable and can be formatted using the standard editing tools, such as Bold, Underline, Font Color, Highlighting, Text Placement, Bulleted List, and so on.

External URL This field displays only when **URL** is selected. Enter the complete path to the external web page that contains the privacy policy that displays when a user logs in to the captive portal.

- From the right of the **Social App Details** option, select the arrow to expand the section. Enter the application IDs and application secrets you received from your social media service providers when you registered your captive portal with them. Facebook™, Twitter™, and Google Plus™ are supported. Enabling these options lets your users log in to the captive portal using their credentials from their social media accounts.

The screenshot shows the 'Social App Details' configuration page. At the top, there are navigation tabs: 'TEMPLATES', 'SMS GATEWAY', 'PREFERENCES' (which is selected and underlined), and 'GUEST USERS'. Below the tabs, the page is organized into sections: 'Terms And Conditions', 'Privacy Policy', and 'Social App Details'. Under 'Social App Details', there are three social media providers listed: Facebook, Twitter, and Google Plus. Each provider has a sub-section with a link to 'How to get the My [Provider] App details?'. Below each link are two input fields: 'APP ID' and 'APP Secret'. At the bottom left of the form, there is a purple 'SAVE' button.

Figure 139: Social Apps Details Configuration

- 6 On the social media site that you are configuring, you must set a redirect/callback URL as follows:

Facebook -

- Under **Client OAuth Settings**:
 - Enable **Client OAuth login**
 - Enable **Web OAuth login**
 - Enable **Embedded Browser OAuth login**
 - Set the **Valid OAuth redirect URI** to <https://cp.ezcloudx.com/auth/facebook/callback>
- Under **Advanced Settings**, enable **Native or Desktop App**

GooglePlus -

- Set the **Authorized JavaScript origins** to <https://cp.ezcloudx.com>
- Set the **Authorized redirect URI's** to <https://cp.ezcloudx.com/auth/google/callback>
- Enable Google Plus API access

Twitter - Set the **Callback URL** to <https://cp.ezcloudx.com/auth/twitter/callback>

- 7 From the right of the **MAC Auth Configuration**, select the arrow to expand the section. Enabling this option lets you set the number of days that the MAC address of a device (which is used during authentication) is retained in the ExtremeCloud database. This lets the user be authenticated automatically and granted immediate access. **Maximum Limit:** 30 days.

The screenshot shows the 'Captive Portal Configurations' interface with the 'PREFERENCES' tab selected. Under the 'MAC Auth Configuration' section, the 'Disable' radio button is selected, and the 'MAC Auth Duration(days)' dropdown menu is set to '30'. A purple 'SAVE' button is located at the bottom of the configuration area.

Figure 140: MAC Authorization Configuration

- 8 Select **Save**.

Next, [configure guest user accounts](#) if needed. Otherwise, [configure a network to use the built-in captive portal](#) and then [assign the network to a site that is configured with the built-in captive portal](#).

Upload Multiple Preconfigured User Accounts

You can configure one or more guest user accounts that are authorized to use the captive portal. This option lets you upload a list of preconfigured users from a CSV (comma separated value) file.



Note


Alternatively, you can [create individual guest user accounts](#).

To upload multiple preconfigured user accounts:

- 1 From the left menu, select **Configure > Policy > Captive Portal**.
- 2 From the **Guest Users** tab, select **Upload CSV**.

The **Upload Guest Wi-Fi Users** dialog opens.

Figure 141: Upload Guest Wi-Fi Users Dialog

- 3 (Optional) If you do not already have a CSV file, select **Click here to download a sample guest Wi-Fi users CSV file** to download a template. Create your own file.
- 4 Select . Select the CSV file from your local file navigation window.
- 5 Select **Save** to upload your guest user accounts.

The **Guest Wi-Fi Users** page displays the list of user accounts.

Status Set an initial status for this account. **Disable** creates the account but not for immediate use. **Enable** creates the account and makes it immediately active.

- 6 (Optional) To edit the account details, select the pencil icon.

Next, [configure a network to use the built-in captive portal](#) and then [assign the network to a site that is configured with the built-in captive portal](#).

Configure a Guest User Account

This option lets you accommodate guests that prefer traditional user-based authentication instead of social app integrated authentication. One account can be assigned to a specific user or one account can be shared by multiple guest users.



Note

Alternatively, you can [upload multiple preconfigured user accounts](#).

To configure a guest account:

- 1 From the left menu, select **Configure > Policy > Captive Portal**.
- 2 From the **Guest Users** tab, select **Add**. Alternatively, select an existing gateway from the list to edit.
- 3 Edit the fields, including username and password. Select a status.

The screenshot shows the 'Captive Portal Configurations' dialog with the 'GUEST USERS' tab selected. Under 'Guest WiFi Users', there are input fields for 'Username' and 'Password'. Below these is a 'Status' section with radio buttons for 'Enable' (selected) and 'Disable'. At the bottom, there is an 'Additional Details' section with a downward arrow, and two buttons: 'SAVE' and 'CANCEL'.

Figure 142: Guest Wi-Fi Users Dialog

Status Set an initial status for this account. **Disable** creates the account but not for immediate use. **Enable** creates the account and makes it immediately active.

- 4 (Optional) Select the arrow to the right of the **Additional Details** section to expand it. If you want to assign the user account to one user, complete the fields. If the account is being used by multiple guests and you want to enforce a network access policy for your organization, you can set just the expiration date without setting the contact information fields.

The screenshot shows the 'Additional Details' section expanded. It contains five input fields: 'First Name', 'Last Name', 'Email', and 'Mobile No.' are arranged in two columns. Below them is an 'Expiry Date (GMT)' dropdown menu with 'Today' selected.

Figure 143: Additional Details Configuration

- 5 Select **Save**.


Next, [configure a network to use the built-in captive portal](#) and then [assign the network to a site that is configured with the built-in captive portal](#).

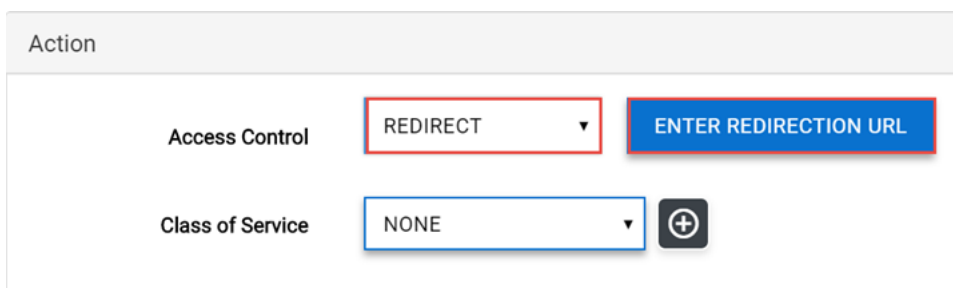
Configure External Captive Portal Redirection

When you configure a third-party or external captive portal, you must configure a policy that:

- Allows access to the captive portal.
- Allows DHCP
- Allows DNS Server
- Allows the IP address range of the default VLAN.
- Redirects at least some HTTP traffic to the captive portal.

To configure external captive portal redirection:

- 1 Select **Configure > Roles > Add** and configure a role. (Alternatively, edit an existing role.)
- 2 For the **Default Action** field, select **Allow**.
- 3 Select  (next to the new rule).
The **Rules** dialog opens.
- 4 Expand the **L3,4** pane.
- 5 Select **New** to add a rule. Set the **Ethertype** to Internet Protocol, version 4 (IPv4). Set the **Port** to HTTP.
- 6 In the **Direction** pane, edit the fields:
 - From User** Specify Destination (dest) as the value.
 - To User** Specify None as the value.
- 7 In the **Access Control** field, select **Redirect**, and then select **Enter Redirection URL** that displays.



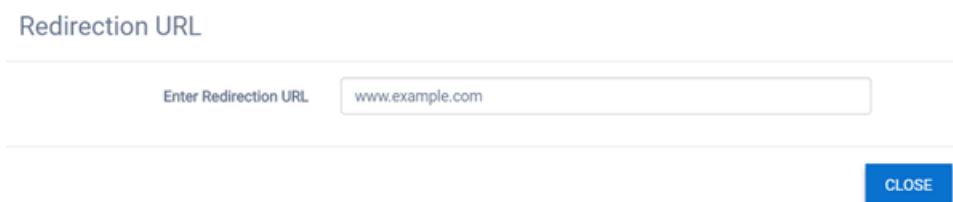
The screenshot shows a configuration window titled "Action". It contains two main sections:

- Access Control:** A dropdown menu is set to "REDIRECT". To its right is a blue button labeled "ENTER REDIRECTION URL".
- Class of Service:** A dropdown menu is set to "NONE". To its right is a grey button with a plus sign (+).

Figure 144: Rules Configuration - Access Control Settings

The **Redirection URL** window opens.

- 8 Enter the URL for the captive portal gateway or select an existing URL from the drop-down list. Select **Close > Close**.



The screenshot shows a window titled "Redirection URL". It features a text input field with the placeholder text "Enter Redirection URL" and the value "www.example.com". A blue button labeled "CLOSE" is positioned at the bottom right of the window.

Figure 145: Redirection URL Configuration

The **Role** configuration page now displays the **Configure Redirect** pane.

- 9 Edit the fields.

Figure 146: Role Configuration

- Identity** Specify the name common to both the AP and the external web server to encrypt the information passed between the AP and the external web server. The identity also tells the receiver which shared secret to use to validate the message signature. If you do not configure the identity, the redirector on the AP drops the traffic.
- Shared Secret** Specify the password that will be used to validate the connection between the AP and the external server. **Limits:** 16 - 225 characters.
- 10 (Optional) [Configure advanced redirection settings](#), which includes specifying a custom URL for the success page after the customer logs in.
- 11 Select **Add Allow Rules**, and enter the IP subnet for the portal.
- 12 Repeat steps 2 - 11 to create a rule that redirects HTTPS traffic. (You must then [configure the advanced redirection settings](#) to enable the **Use HTTPS for User Connection** option.)
- The rule is created and displays in the **Rules** list.
- 13 Add other access control rules as appropriate. Be sure to allow access for DHCP, DNS, and ARP requests.
- 14 Save the role.
- 15 Configure a network by selecting **Networks > Add** or by editing an existing network.
- 16 Select the newly defined role from the **Default Unauth Role** list.
- 17 If needed, make additional changes to the network's configuration.
- 18 Save the network configuration.

Configure Advanced Settings for External Captive Portal

If you plan to use a third-party or external captive portal (ECP), you must configure the redirection URL. The URL can be a custom URL and is supported for all cloud-enabled access points.

- 1 From the **Configure Role** page, you must configure at least one policy rule with a Redirect action to make the **Advanced** option display.

The screenshot shows the 'Configure Role' page for 'Role_1'. Under the 'Configure Redirect' section, the 'Redirect URL' field contains 'http://www.example.com'. A note below it states: 'Note: "token=<integer_val>&dest=<original_target_url>" will be appended to the URL'. The 'Identity' and 'Shared Secret' fields are empty. A note below the 'Shared Secret' field says 'Shared secret should be between 8 - 64 characters'. An 'Add Allow Rules' link is visible next to the URL field. An 'ADVANCED' button is located at the bottom right of the configuration area.

Figure 147: Configure Role page with redirect URL enabled

- 2 Select **Advanced**.
The **External Captive Portal** dialog opens.
- 3 In the **Redirect To External Captive Portal** pane, select the options that you want.

The screenshot shows the 'External Captive Portal' dialog. The 'Redirect to External Captive Portal' section has a sub-section 'Optional items to include in URL' with the following checked options: AP serial number and name, Client MAC address, Network SSID, Network Name, Associated BSSID, Current Role, and Containment VLAN (if any). The 'Redirect from External Captive Portal' section has 'Use HTTPS for User Connection' checked and 'On successful login redirect user to' set to 'ORIGINAL DESTINATION'. A 'CLOSE' button is at the bottom right.

Figure 148: Captive Portal - Advanced Settings

- AP Serial Number and Name** (Optional) Specifies that the name and serial number that is stored locally on the AP will be included in the URL that redirects to the ECP.
- Client MAC Address** (Optional) Specifies that the client's MAC address, if one is being used for authentication, will be included in the URL that redirects to the ECP.

- Associated BSSID** (Optional) Specifies that the Basic Service Set Identifier (BSSID) to which the redirected client is associated will be included in the URL that redirects to the ECP. The (BSSID) is a MAC address belonging to the AP to which the clients will be associated.
- Current Role** (Optional) Specifies that the name of the access control role assigned to the client at the time its browser was redirected to the ECP will be included in the URL.
- Containment VLAN** (Optional) If the default action of the Currently Role is Contain to VLAN, selecting this option will include the name of the VLAN to which the client's traffic is contained in the URL.

- 4 In the **Redirect From External Captive Portal** pane, edit the fields:

Figure 149: Example: Custom URL Configuration

- Use HTTPS for User Connection** (Optional) If the default action of the Currently Role is Contain to VLAN, selecting this option will include the name of the VLAN to which the client's traffic is contained in the URL.
- Send Successful Login To** Specify what the AP should do after the ECP has redirected a successfully authenticated user back to the AP. If **Custom URL** is selected, enter the URL that the role will be directed to from the ECP.
- | | |
|------------------------------------|---|
| Original Destination | The AP redirects the user to the destination it was trying to reach originally when it was redirected for authentication. |
| Captive Portal Session Page | The AP redirects the user to a page that tracks how long they have been online and that has controls to allow the user to terminate their session explicitly. |
| Custom URL | The AP redirects all successfully logged in clients to a URL that you want your clients to start their session, such as your company's announcements page. |

- 5 Select **Close**.
- 6 On the **Configure Role** page, select **Create Rule > Save**.

Create a Walled Garden

A walled garden can be created for a captive portal to control access to Web content and services. A walled garden is often used in hotel environments. Unauthenticated users are given access to a designated login page and all of its allowed contents. When the unauthenticated user attempts to navigate to other websites that are not whitelisted in the walled garden profile, they are redirected to the login page.

To create a walled garden:

- 1 **Configure a network service** to use either the built-in captive portal feature or a third-party captive portal in the **Captive Portal** field.
The **Walled Garden DNS Whitelist** button displays.
- 2 Select **Walled Garden DNS Whitelist** and add at least one fully qualified domain name (FQDN) to the whitelist.

How to Limit Bandwidth

This process describes the workflow of how to limit bandwidth and test that it is working.

- 1 Create a role that limits bandwidth.
- 2 Create a network and assign it to the limited bandwidth role.
- 3 Create an Allow All role that does not limit the bandwidth.
- 4 Create a second network and assign the Allow All role to that second network.
- 5 Assign **both** networks to a site.
- 6 Test the SSID on a mobile phone using an application that measures speed, such as the Netflix FAST app. Make sure that you choose an application that your network policy allows.
 - 1 Log in to the Allow All network.
 - 2 Open the application to test the Wi-Fi speed. You should see the bandwidth speed is unlimited (at the maximum speed to which your network service is contracted).
 - 3 Log in to the Limited Bandwidth network.
 - 4 Open the application to test the bandwidth speed. Your speed is limited to the Mbps speed that you configured in your policy.

14 Tools

Port Manager Overview
Use Packet Capture
Use Ping and Trace Route
Use the Wireless Debug Tool

The following tools and procedures are available:

- [Use Port Manager](#) on page 203
- [Use Packet Capture](#) on page 205
- [Use Ping and Trace Route](#) on page 207
- [Use the Wireless Debug Tool](#) on page 208

Port Manager Overview

The Port Manager feature lets you virtually configure all of your switch ports as if they belonged to one switch, similar to virtual stacking. The switches can be in different physical locations and can be of different model types.



Note

To manage an individual switch port, see [Configure an Individual Port](#) on page 152

Using Port Manager, you can find all the ports across the network using search criteria (such as those on the same VLAN, site, or category), and then edit the entire group of ports. Some of the actions that you can perform with Port Manager are:

- Filter the Port Manager display, for example, to view all ports on a controlling bridge (including VPEX)
- Assign or delete one or more categories assigned to the selected port or ports (such as VoIP or IoT)
- Assign or delete one or more VLANs (topologies)
- Assign or delete one or more VLAN groups (topology groups)
- Modify the PVID
- Assign a port function (Interswitch, Host, AP, Other) to selected ports
- Create a LAG for ports that are on the same switch



Note

AP ports cannot have VLANs removed if they are required by AP services.

ExtremeCloud lets you apply multiple categories (labels) to help you manage groups of ports logically. Categories can be user-defined to reflect the logical classification used by your organization. For example, you can categorize ports primarily by location and then apply a further level of classification using categories such as WLAN or PoE to identify ports for wireless access points.

When you perform a search, you can combine filter criteria and then sort the results by selecting the column headers.

A port function cannot be deleted, but it can be assigned **Other** if another function is not appropriate.

VLANs are topologies. VLAN groups are topology groups that can be created and assigned to a group of ports, and more than one VLAN group can be assigned to a port.

A VLAN can be used in more than one VLAN group.

Each VLAN group is treated as one entity. A VLAN group can also contain VLANs that have more than one VLAN ID assigned to it.

Audit logs are created for all configuration changes and can be viewed under **Admin > Audit Logs > .**

More Information

- [Use Port Manager](#) on page 203

Use Port Manager

The Port Manager feature lets you configure all of your switch ports as if they were one switch, similar to virtual stacking. The same configuration can be pushed to a large number of ports on the same or multiple switches. The switches can be in any physical location and can be of different model types.

One advantage of Port Manager is that it clearly differentiates port usage. For example, controlling bridges with MLAGs can have multiple copies of a port. Port Manager flattens out the view so that instead of looking like several copies of a port, the port displays as differentiated ports with aliases.

AP ports cannot have VLANs removed if they are required by AP services.



Note

To manage an individual switch port, see [Configure an Individual Port](#) on page 152

To configure multiple ports with the same configuration:

- 1 Select **Tools > Ports**

- In the **Filter By** pane, select one or more search criteria by which you want to search, and select **Filter**.

The list of results display below the **Filter By** pane.

<input checked="" type="checkbox"/>	Switch and Port	Name	Categories	Site	VLAN IDs	Status	Type
<input type="checkbox"/>	1000G-00000(1)	1		Default	1	On	Other
<input type="checkbox"/>	1000G-00000(2)	2		Default	1	On	Other
<input checked="" type="checkbox"/>	1000G-00000(3)	3		Default	1	On	Other
<input type="checkbox"/>	1000G-00000(4)	4		Default	1	On	Other
<input type="checkbox"/>	1000G-00000(5)	5		Default	1	On	Other
<input checked="" type="checkbox"/>	1000G-00000(6)	6		Default	1	On	Other
<input checked="" type="checkbox"/>	1000G-00000(7)	7		Default	1	On	Other
<input type="checkbox"/>	1000G-00000(8)	8		Default	1	On	Other
<input checked="" type="checkbox"/>	1000G-00000(9)	9		Default	1	On	Other
<input type="checkbox"/>	1000G-00000(10)	10		Default	1	On	Other

Figure 150: Port Manager Filtering


- (Optional) Change the number of results that display on the page using the **Records per page** drop-down list.
- (Optional) Sort the list using the **Sort By** drop-down list, and deselect any switches that you want to exclude from any new configuration changes.
- (Optional) Select  display the options menu for exporting the data or to managing which columns display.
- In the **Actions** pane, configure one or more actions from the drop-down lists:

Figure 151: Port Manager Actions

VLANs (Optional) Select either **Assign** or **Delete** to assign a VLAN topology. When you select one of these options, a secondary drop-down list displays a list of available VLANs. Select one or more VLANs to assign or delete. A VLAN can be used in more than one VLAN group.

VLAN Groups (Optional) VLAN Groups are topology groups that contain one or more VLAN IDs. VLAN groups can be assigned to a port or a group of ports, and each port can have more than one VLAN group assigned to it. Each VLAN group is treated as one entity. A VLAN group can also contain VLANs that have more than one VLAN ID assigned to it.

PVID	(Optional) Specify the Port VLAN ID (PVID) that will be assigned to the access ports by default. Use caution with this setting as it can isolate your port.
Categories	Select Assign or Delete . From the drop-down list the displays, select the categories you want to add or remove from the selected ports.
Port Function	(Optional) Assign a function for the port (Interswitch, Host, AP, Other). We do not recommend changing AP ports to another function, however it can be changed to Other if needed.
LAG	(Optional) Select Combine to display the Master Port drop-down list. Select a port from the list to assign the selected switches to a master port.
Admin State	(Optional) Select On or Off to enable reporting on the state of the ports.
Port Speed	Set the port speed to Auto , 1G , 10M , or 100M . 1G is typically a small form factor pluggable (SFP) fiber port. 10M and 100M are copper ports. Auto specifies that the port will automatically negotiate the port speed.
Port Duplex	Set the port duplex setting to Full or Half . Half duplex means that frames can only flow in one direction at a time. Full duplex allows frames to flow in both directions at the same time.
Energy Efficient Ethernet	When enabled, this setting reduces power consumption during periods of low data activity.

7 Select **Submit**.

Your configuration changes are saved and pushed to the selected switch ports.

Use Packet Capture

The Packet Capture tool is available for ExtremeWireless WiNG access points (APs) at the site level or at the individual device level. The tool captures information about network traffic to assist with forensics (such as detect misuse of the network by internal or external users) and help troubleshoot network problems (such as utilization of network resources).

To capture packet information:

- From the menu on the left, do one of the following:
 - Select **Tools > Sites**. Select a site from the list that displays. You will be able to capture information for all APs or for a single AP at the site.
 - Select **Tools > Access Points**.

- 2 Select the **Packet Capture** tab.

Figure 152: Packet Capture Tab

- 3 In the **Capture Locations** drop-down list, select the packet types to capture.

All Wired Packets	Captures all packets from the different wired ports. Packets are captured from both directions.
Dropped	Captures all packets that were dropped due to various reasons, such as ACLs and timeouts.
Wired	Captures packets from a specified wired interface. Select the interface type and interface number from the drop-down list. From the Packet Direction drop-down list, select the packet flow direction (Any, Inbound, or Outbound).
Wireless	Captures packets from a specified wireless radio interface. Select the interface from the drop-down list of available radios for the access point. From the Packet Direction drop-down list, select the packet flow direction (Any, Inbound, or Outbound).

- 4 In the **Filter** section, select one or more filter criteria for which you want to capture packets. Packets are captured only for the options you select.

MAC Address	Enter a device's MAC address for which packets will be captured. All other packets are filtered out.
IP Protocol	Select a protocol from the drop-down list for which packets will be captured. All other packets are filtered out.
Filter by IP	Enter a device's IP address for which packets will be captured. All other packets are filtered out.
Port	Set the port number for which packets will be captured. All other ports are filtered out.

- 5 In the **Maximum Packet Count** field, set the maximum number of packets that you want to capture. Use the **Save to Disk** option to download a PCAP file.



Note

The maximum data capture limit is 500 MB. A maximum of 5,000 packets can be seen in the user interface. The maximum capture count is 200,000 packets that can be captured and downloaded using a PCAP file.

6 Select **Start**.

Packet information displays in the **Details** pane. You can save the information files to your local file system. The files are not retained in ExtremeCloud after you log out.

**Note**

To stop the tool, select **Stop**. The information display pane shows the packets that were captured before stopping, and the packets can be downloaded using the **Save to Disk** option.

Use Ping and Trace Route

The Ping and Trace Route tools work with ExtremeWireless WiNG APs to help to troubleshoot network connection issues on an access point (AP). These operations can only be performed for online devices.

Ping tests whether a host can be reached on an IP network and measure the round trip time from the originating host to its destination and back again.

Trace Route displays a route (path) and measures the delays for packets traversing the network. The history of the route is recorded as the round trip time a packet is received at each successive host in the route. The sum of the mean time to each host is the total time required to establish the remote connection to the remote host.

To use ping and trace route:

- From the menu on the left, do one of the following:
 - Select **Tools > Sites**. Select a site from the list that displays. You will be able to capture information for all APs or for a single AP at the site.
 - Select **Tools > Devices > Access Points**. Select an AP and then select **Tools** from the AP details page. Packet information is captured only for the selected AP.
- Select the **Ping Trace** tab.

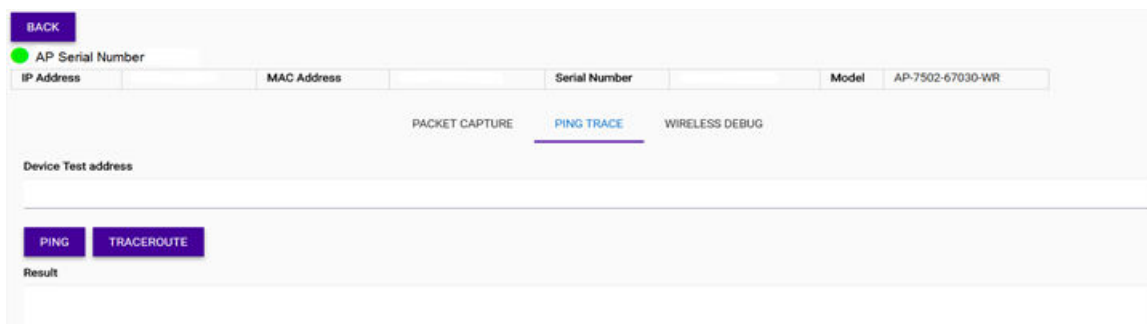


Figure 153: Ping Trace Tab

- In the **Device Test Address** field, enter the IP address of the device to ping or trace. Only IPv4 addresses are supported.
- To ping the IP address, select **Ping**. To trace the packet path to the defined IP address, select **Traceroute**.

The results display in the **Result** pane.

Use the Wireless Debug Tool

Enable the Wireless Debug tool to capture events at the site level for ExtremeWireless WiNG access points (APs) and to troubleshoot performance issues. You can also use the information to preempt potential network threats.

- From the menu on the left, do one of the following:
 - Select **Tools > Sites**. Select a site from the list that displays. You will be able to capture information for all APs or for a single AP at the site.
 - Select **Tools > Devices > Access Points**. Select an AP and then select **Tools** from the AP details page. Packet information is captured only for the selected AP.
- Select the **Wireless Debug** tab.

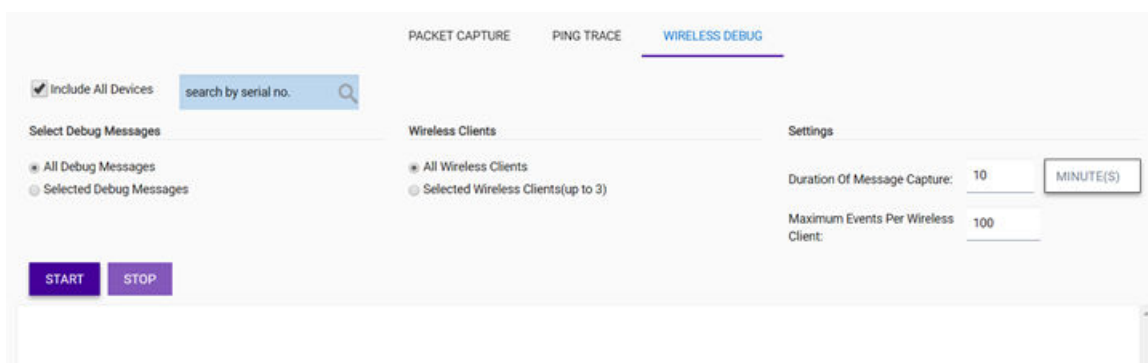


Figure 154: Wireless Debug Tab

- For the **Include All Devices** option, you can use the default option to capture wireless information for all devices as they roam through the site. To capture information for a specific device in the site, disable the option and then search for the device's serial number in the search box that displays when you select that option.
- In the **Select Debug Messages** section, specify the types of messages that you want to capture:

All Debug Messages	Captures all wireless debug messages.
Selected Debug Messages	Enable this option to filter messages using one or more of the filter options. (The filters display when this option is enabled.) Using multiple filters gives more insight to troubleshooting.
802.11 Management	Logs WLAN IEEE 802.11 connection (login/logout) event messages. This filter helps to troubleshoot mobility and SMART client load balancing issues.
EAP	Logs EAP authentication messages. This filter helps to troubleshoot events related to client authentication issues during roaming.
Flow Migration	Logs migration flows of wireless clients between access points within the specified site. This filter helps to troubleshoot roaming issues.
RADIUS	Logs RADIUS server authentication event messages. This filter helps to troubleshoot connectivity issues between the access points and RADIUS servers.
System Internal	Logs internal system debug messages. This filter helps to troubleshoot system issues.

WPA/WPA2 Logs WPA/WPA2 authentication and encryption event messages. This filter helps to troubleshoot 4-way handshake issues during initial association, re-authentication, or roaming.

- 5 In the **Wireless Clients** section, specify the wireless clients for which logs will be captured.
 - All Wireless Clients** Captures debug messages for all wireless clients for the specified site.
 - Selected Wireless Clients** Captures debug messages for up to three individual client MAC addresses. Enter the MAC addresses in XX-XX-XX-XX-XX-XX format.
- 6 In the **Settings** section, specify the capture duration and the maximum number of events to capture for each wireless client.
 - Duration of Message Capture** Specify the duration in either hours, minutes, or seconds. **Default:** 10 minutes.
 - Maximum Events Per Wireless Client** Specify the maximum number of debugs to capture for each client. **Limit:** 1 - 10,000 **Default:** 100
- 7 To start the wireless debug log capture, select **Start**.

**Note**

To stop the log capture, select **Stop**.

The results display in a list.

- 8 To save the log files to your local hard drive, select **Save to Disk**.
- 9 To hide the configuration section of the **Live Wireless Debug Events** page, select **Hide Capture Options**.

15 Reports

Create Templates and Run Reports
Run PCI Compliance Reports
Run Security Reports
View Scheduled Reports
View Generated Reports
View Audit Log Files

You can create customized report templates using the template builder.

There are also the following predefined templates:

- [PCI Compliance Report](#)
- [Security Report](#)

Most reports templates can be created with any combination of type, scope and period parameters. The exception is the Security Report, which is always scoped to the full tenant configuration, and the period is irrelevant as it only looks at the current database configuration.

Reports can be scheduled to have periodic data for further analysis. Use the reports to have a record of the performance of the networks managed by a tenant, and to tune the network for better performance or for troubleshooting. Detailed reports enable network administrators to view attempted intrusions into their networks and to have insight into the activities of their clients.

Reports are stored for one month and can be emailed to a distribution list. (Stored reports can also be deleted manually.) The report output formats are PDF and CSV.

More Information

- [Create Templates and Run Reports](#) on page 211
- [Run PCI Compliance Reports](#) on page 213
- [Run Security Reports](#) on page 216
- [View Scheduled Reports](#) on page 219
- [View Generated Reports](#) on page 219

Create Templates and Run Reports

Use the **Templates** page to create, edit, run, or delete custom reports. You can customize reports to suit specific report data capture requirements.



Note

You can also run predefined reports for **PCI compliance** and **security** from the Templates page using the templates with those names. The predefined reports are not customizable.







Reports are created from templates by using the scheduler. The scheduler can be configured to generate the report once, immediately, or it can request that the report be run periodically.

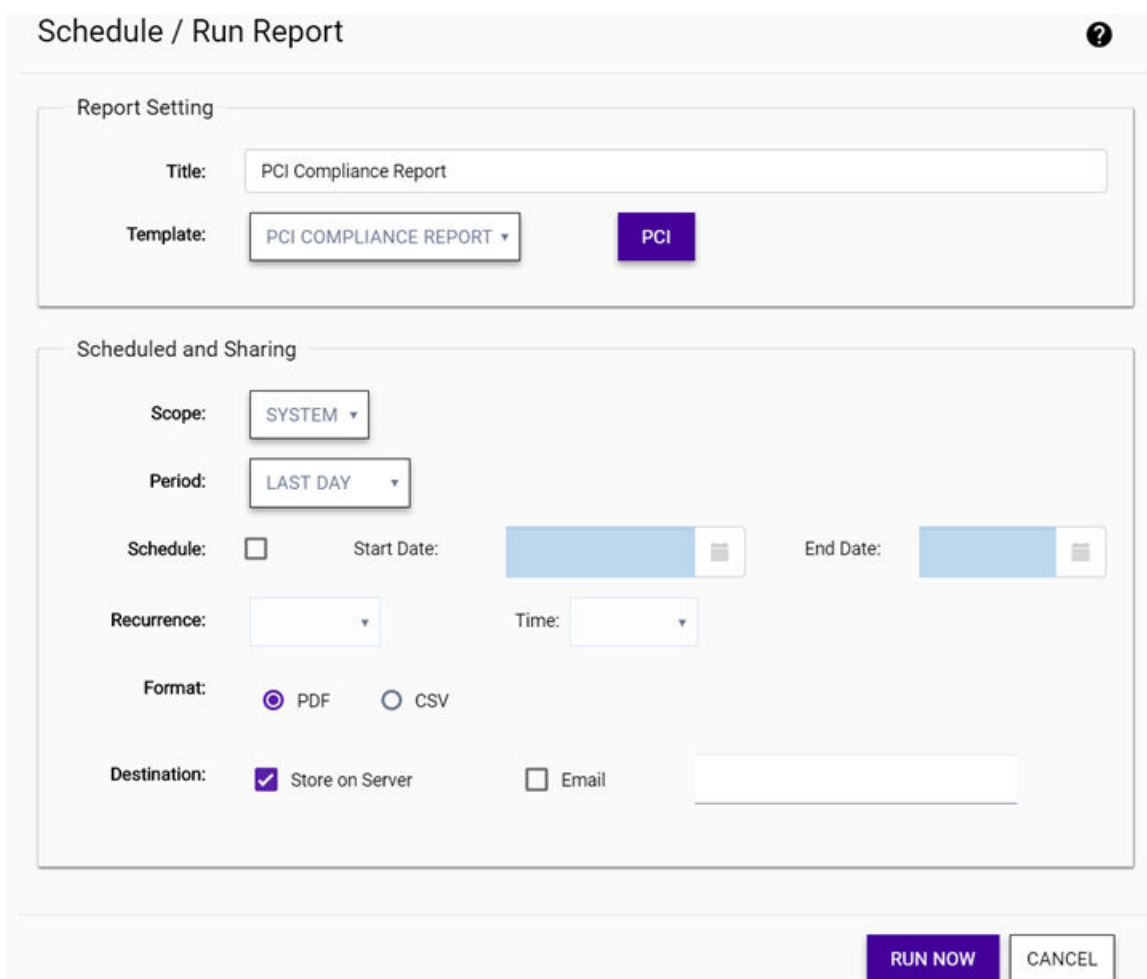
To create a template and schedule a report:

- 1 From the main menu, select **Reports**.
The reports page opens and displays a list of templates.
- 2 On the default **Templates** page, select **Add**.
The **Create Template** page opens.

Figure 155: Create Report Template

- 3 In the **Name** field, enter a name for the report.
- 4 From the right menu, drag and drop one or more content types that you want to include in the report to the **Report Title** pane.
- 5 Select **Save**.
Your report is saved. The list of report templates are displayed automatically and your new report is included in the list. templates.
- 6 To schedule a report, select a report name in the **Templates** list.
A group of management icons display to the left of the report name.

- 7 Select an icon to make changes to, clone, or delete the template. For the PCI Compliance and Security reports, the **Schedule** option is the only available option.
-  - View the configuration details of the selected report template.
 -  - Edit the configuration of the selected report template.
 -  - Copy the selected report template to save effort in creating a similar report, and then make changes to the copied template.
 -  - Schedule the selected report template to run a report.
 -  - Delete the selected report template.
- 8 To schedule a report to run, select .
The **Schedule/Run Reports** dialog opens.



Schedule / Run Report

Report Setting

Title: PCI Compliance Report

Template: PCI COMPLIANCE REPORT **PCI**

Scheduled and Sharing

Scope: SYSTEM

Period: LAST DAY

Schedule: Start Date: [] End Date: []

Recurrence: [] Time: []

Format: PDF CSV

Destination: Store on Server Email []

RUN NOW **CANCEL**

Figure 156: Schedule / Run Report Dialog

- 9 Edit the fields, and select **Run Now**.
- Title** Enter a report title to apply significance to the data that is captured.

- Template** Select the report template that you want to run from the drop-down list. This list includes the Security report template, the PCI Compliance report template, and any custom report templates for your organization.
- Scope** Specify the scope as **System** to generate a report for the whole system, including each configured network. Otherwise, select a network from the drop-down list to restrict the report to the selected network.
- Period** Specify the reporting period (Last Hour, Last Day, Last Week, Last Month). These are not relevant for the Security report.
- Schedule** To schedule the report generation, select the **Schedule**, and then specify a start date and end date using the calendar function. The report will only run on or after the date set in the **Start Date** field. The report will not run after the date set in the **End Date**. If you do not select the **Schedule** check box, the report will run as soon as it is submitted and it run only once.
- Recurrence** (Optional) Specify the recurrence frequency and the time this report is run, either daily, weekly, or monthly.
- Daily** Runs the report daily. Use the **Time** drop-down menu to set the time at which to run the daily report.
 - Weekly** Runs the report on a particular day of the week. Use the **Day of Week** field to set the weekday to run the report on. Use the **Time** drop-down menu to set the time the weekly report is generated.
 - Monthly** Runs the report on a particular date of the month, every month. Use the **Day of Month** field to set the date. Use the **Time** drop-down menu to set the time to begin the historical report data gathering process.
- Format** Specify the output format for this report: PDF or CSV.
- Destination** Select a destination option to configure how a generated report is stored:
- Store on Server** Select this check box to stores and archive a generated report on the server. Generated reports are listed on the **Generated Reports** tab.
 - Email** Select this check box to send the report by email. In the adjoining text box, enter one or more email addresses (separated by commas) to which the report will be sent.

The report is run at the configured interval. The generated report is available from the **Generated Reports** page.

Run PCI Compliance Reports

PCI Compliance reports list the compliance status of the Payment Card Industry (PCI) Data Security Standard parameters. The information in these reports are used by vendors to prove compliance to credit card companies and identify areas where they need to make changes in order to be compliant.

You can define, schedule, download, and delete PCI reports, and configure reports to be sent to a list of email addresses.

These reports can be requested for an entire tenant or for a specific tenant site.

If you have a site with ExtremeWireless WiNG APs, the PCI compliance report also contains a Threat AP information section.

To run a PCI compliance report:

- 1 From the main menu, select **Reports**.
The reports page opens and displays a list of templates.
- 2 Select the PCI Compliance template from the list.

The Schedule button (📅) displays.

- 3 To schedule a report to run, select 📅.
The **Schedule/Run Reports** dialog opens.

Schedule / Run Report

Report Setting

Title: PCI Compliance Report

Template: PCI COMPLIANCE REPORT **PCI**

Scheduled and Sharing

Scope: SYSTEM

Period: LAST DAY

Schedule: Start Date: [Date Picker] End Date: [Date Picker]

Recurrence: [Dropdown] Time: [Dropdown]

Format: PDF CSV

Destination: Store on Server Email [Text Field]

RUN NOW **CANCEL**

Figure 157: Schedule / Run Report Dialog

- 4 Edit the fields.

Title Enter a report title to apply significance to the data that is captured.

Template From the drop-down list, select **PCI Compliance Report**. Select the **PCI** button that displays.

The **PCI Details** dialog opens.

PCI Details

Figure 158: PCI Details Dialog

- 5 In the **General Settings** pane, edit the fields.

Secured Cardholder Data Environment (CDE) Network	Specify whether to include the Cardholder Data Environment (CDE) networks when creating the report.
CDE WLANs	From the drop-down list, select the WLANs to include when generating the report. Use the Search box to find WLANs if the list is long.
All access points are physically secured	When enabled, the report indicates that all access points are verified as being physically secured.
- 6 In the **Accounts** and **Password** panes, enable the options that reflect how your environment is set. The options include:
 - Each user has his/her own user ID
 - Accounts that are inactive for more than 90 days are suspended
 - Vendor accounts are active only when needed
 - The accounts of terminated users are revoked
 - Password contains both numeric and alphabetic characters
- 7 Select **Save**.
You return to the **Schedule/Run Report** dialog.

8 Edit the remaining fields.

- Scope** Specify the scope as **System** to generate a report for the whole system, including each configured network. Otherwise, select a network from the drop-down list to restrict the report to the selected network.
- Period** Specify the reporting period (Last Hour, Last Day, Last Week, Last Month). These are not relevant for the Security report.
- Schedule** To schedule the report generation, select the **Schedule**, and then specify a start date and end date using the calendar function. The report will only run on or after the date set in the **Start Date** field. The report will not run after the date set in the **End Date**. If you do not select the **Schedule** check box, the report will run as soon as it is submitted and it run only once.
- Recurrence** (Optional) Specify the recurrence frequency and the time this report is run, either daily, weekly, or monthly.
- Daily** Runs the report daily. Use the **Time** drop-down menu to set the time at which to run the daily report.
 - Weekly** Runs the report on a particular day of the week. Use the **Day of Week** field to set the weekday to run the report on. Use the **Time** drop-down menu to set the time the weekly report is generated.
 - Monthly** Runs the report on a particular date of the month, every month. Use the **Day of Month** field to set the date. Use the **Time** drop-down menu to set the time to begin the historical report data gathering process.
- Format** Specify the output format for this report: PDF or CSV.
- Destination** Select a destination option to configure how a generated report is stored:
- Store on Server** Select this check box to stores and archive a generated report on the server. Generated reports are listed on the **Generated Reports** tab.
 - Email** Select this check box to send the report by email. In the adjoining text box, enter one or more email addresses (separated by commas) to which the report will be sent.

9 Select **Run Now**.

The report is generated and sent to the destination you have configured.

Run Security Reports

A network security report:

- Shows you the percentages of services that are insecure
- Describes the security weaknesses
- Provides guidance about how to mitigate each weakness

Threats that are included in this report are:

- Open networks
- SSIDs that are the same as or similar to SSIDs targeted by honeypot tools
- WPA PSK keys that are easy to decode either because they are too short or are publicly available in rainbow tables

To view a security report:

- 1 From the main menu, select **Reports**.
The reports page opens and displays a list of templates.
- 2 On the **Templates** page, select **Security Report**.

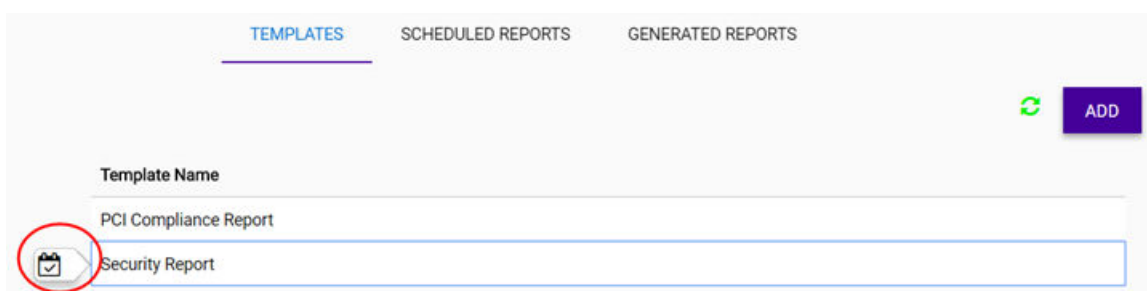


Figure 159: Security Report Template and Scheduling Button

- The scheduling button (📅) displays.
- 3 Select 📅.
The **Schedule/Run Report** dialog opens.
- 4 To schedule a report to run, select 📅.
The **Schedule/Run Reports** dialog opens.

Figure 160: Schedule / Run Report Dialog

- 5 Edit the fields, and select **Run Now**.

Title Enter a report title to apply significance to the data that is captured.

Template Select the report template that you want to run from the drop-down list. This list includes the Security report template, the PCI Compliance report template, and any custom report templates for your organization.

Scope Specify the scope as **System** to generate a report for the whole system, including each configured network. Otherwise, select a network from the drop-down list to restrict the report to the selected network.

Period Specify the reporting period (Last Hour, Last Day, Last Week, Last Month). These are not relevant for the Security report.

Schedule To schedule the report generation, select the **Schedule**, and then specify a start date and end date using the calendar function. The report will only run on or after the date set in the **Start Date** field. The report will not run after the date set in the **End Date**. If you do not select the **Schedule** check box, the report will run as soon as it is submitted and it run only once.

Recurrence (Optional) Specify the recurrence frequency and the time this report is run, either daily, weekly, or monthly.

- Daily** Runs the report daily. Use the **Time** drop-down menu to set the time at which to run the daily report.
- Weekly** Runs the report on a particular day of the week. Use the **Day of Week** field to set the weekday to run the report on. Use the **Time** drop-down menu to set the time the weekly report is generated.
- Monthly** Runs the report on a particular date of the month, every month. Use the **Day of Month** field to set the date. Use the **Time** drop-down menu to set the time to begin the historical report data gathering process.

Format Specify the output format for this report: PDF or CSV.

Destination Select a destination option to configure how a generated report is stored:

- Store on Server** Select this check box to store and archive a generated report on the server. Generated reports are listed on the **Generated Reports** tab.
- Email** Select this check box to send the report by email. In the adjoining text box, enter one or more email addresses (separated by commas) to which the report will be sent.

The report is run at the configured interval. The generated report is available from the **Generated Reports** page.

View Scheduled Reports

You can view list reports that are scheduled to run at a future point of time.

- 1 From the main menu, select **Reports**.
The reports page opens and displays a list of templates.
- 2 Select the **Scheduled** tab.
The list of scheduled reports displays.
- 3 (Optional) To delete a scheduled report, select a report from the list and select **Delete**.
The scheduled report is deleted.

View Generated Reports

By default, there are no existing reports until you create and schedule reports. After the reports are generated, you can filter them for each configured network.

To view reports:

- 1 From the main menu, select **Reports**.
The reports page opens and displays a list of templates.
- 2 Select **Generated Reports**.
The **Generated Reports** tab displays a list of generated reports and information about the scope of the report, including the following information:
 - Report** Displays the name of the report as a link. Select the link to view the details of the report in a separate window.
 - Category** Describes the report content type.

- User** Displays the email address of the user who created the report.
- Start Date** If configured, displays the start date of the report contents.
- End Date** If configured, displays the end date of the report contents.
- Run On** Displays the date and time when this report was run last. Use this information to determine the report's current relevance.
- Action** Use the icons to view, save, or delete the report in that row or refresh the page.

View Audit Log Files

All configuration changes made by administrators are logged. You can view a record of the configuration changes in the user interface.

Audit log files include the following information:

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

To view audit log files:

- 1 Select **Reports > Audit Logs** from the menu.

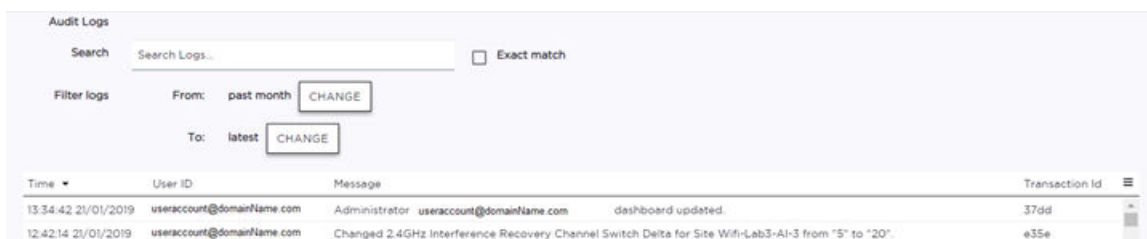



Figure 161: Audit Logs Page

The **Audit Logs** page opens.

- 2 (Optional) Enter text to search for a specific audit log. If needed, select the **Exact Match** check box.
- 3 Set a filter or use the default filter.
- 4 Select **Enter** to execute a search.

The audit log list is updated.

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

16 Administration

Create, Modify, or Disable Administrator Accounts
Delete Administrator Accounts
Configure General System Settings
Configure Email Notifications
Assign Switch Licenses

The **Administration** section of the user interface lets administrators manage accounts, set up email notifications, configure enhanced global security, access audit logs, and assign switch license vouchers.

Email notifications are managed by navigating to **Administrations > Accounts**.

More Information

- [Create, Modify, or Disable Administrator Accounts](#) on page 221
- [Delete Administrator Accounts](#) on page 224
- [Configure Email Notifications](#) on page 227
- [View Audit Log Files](#) on page 220
- [Configure General System Settings](#) on page 224
- [Assign Switch Licenses](#) on page 228

Create, Modify, or Disable Administrator Accounts

The first administrator account created is a Power Administrator with full privileges, and can create additional power administrators, administrators with read/write privileges, and accounts with read-only privileges. For more information about the access types and roles, see the field description that follows for **Access Level**.

When a new account is created using email validation, the account displays on the **Accounts** page in the **Not Activated** state. The user is sent an email with a link to complete the activation. **Enabled** indicates that the account is active.

This procedure also lets you disable accounts. You can disable this option to suspend the account while preserving the account record. Disabling can be useful when an employee is on temporary leave and is expected to be reinstated at a later date.

- 1 Select **Administration > Accounts** from the menu.
- 2 To create a new account, select **Add**. To modify or disable an existing account, select an account from the list and edit the details.

- 3 Edit the fields.

The screenshot shows a configuration form for administrator accounts. The fields are as follows:

- E-mail Address:** A text input field containing the example "user@company.com".
- Access Level:** A dropdown menu currently set to "READ/WRITE".
- Password:** A text input field with the placeholder "Enter a password".
- Confirm Password:** A text input field with the placeholder "Re-enter the password".
- Security Question:** A text input field with the placeholder "Enter a security question".
- Security Question Answer:** A text input field containing "Answer". Below this field is a red error message: "A security question answer is required".
- Idle timeout (minutes):** A text input field containing the value "5".
- Two-step Verification Enabled:** A checkbox that is currently unchecked.

Figure 162: Administrator Accounts Configuration

Admin Role Define the type of administrator role based on the privileges you want to grant.

Access Level Assign the access level for the account:

Read-only The account has read-only privileges.

Read/Write The account is an Administrator role with read and write privileges.

Power Admin The account is a Power Administrator role with the ability to create additional accounts with any role or access level.

Security Question and Answer Enter a customized question and answer.

Idle Timeout Specify an inactivity timeout value between 1 - 1440 minutes.

Enabled This attribute displays after the account creation is validated. After validation, initially the account is in a **Not Activated** state. The user is sent an email with a link to complete the activation. **Enabled** indicates that the account is active. You can disable the account, such as when an employee is on temporary leave.

- 4 (Optional) Enable two-step verification (2FA) for increased security. This feature lets you either manually enter back-up codes use the Google Authenticator app to generate a code. The backup code must be entered during login, in addition to the account password.

- 5 (Optional) Enable or disable email notifications.

e-Mail Notifications

Upgrade Scheduled Device Group Upgrade Started Device Group Upgraded

Configuration Changed Device Status Changed

Figure 163: Email Notification Configuration

- 6 Select **Save**.

Your account settings are saved and, if you selected two-step verification, the Google Authenticator pane displays a QR code and backup code generation.

- 7 To complete configuration of two-step verification, generate the backup codes and store them securely, and download the Google Authenticator app to your Apple or Android mobile device.

Select  to export the data to CSV and manage which columns display.




Important

The backup codes are intended for use if the administrator loses the device that has the Google authenticator application and configuration.

Google Authenticator

Google Authenticator generates 2-step verification codes on your phone. Enable 2-step verification to protect your account from hijacking by adding another layer of security. With 2-step verification signing in will require a code generated by the Google Authenticator app in addition to your account password.

Show backup codes

Code	Available	
17020737		Export all data as csv
17836617		Export visible data as csv
26409204		Columns:
26501574		<input checked="" type="checkbox"/> Code
41076053		<input checked="" type="checkbox"/> Available
47075112		
52949721	true	
68533642	true	
70196166	true	
87693259	true	

GENERATE NEW BACKUP CODES

Figure 164: Back-up Codes

- To use backup codes for account verification:

- 1 Select **Show backup Codes**.
 - 2 Export the backup codes to a CSV file and store them in a safe place. (These codes can also be used if you are using the Goggle Authenticator app and your mobile device becomes unavailable).
 - 3 Generate additional backup codes when needed. Each back-up code can be used only once. After a code is used, its status changes from **true** to **false**.
- To enable the Google Authenticator app, do one of the following steps:
 - Select the scanning option in the app, and then scan the QR code that displays in the ExtremeCloud user interface.
 - In the mobile app, choose the option to enter keys manually. By default, **Time Based** is enabled and it is the **only** supported option.



Important

Do **not** select "Counter Based" because the account will be locked and the user will not be able to retrieve the account from the **Forgot Password** link.

Your mobile device is enabled to use the Google Authenticator app to generate a log in code for ExtremeCloud. (Each code generated by the app expires after 30 seconds. Generate a new code and enter it manually each time you log in.)

Delete Administrator Accounts

A Full Administrator can delete any other administrator account. This action permanently deletes the user account and its record. However, the last Full Administrator account cannot be deleted or disabled.



Note

Consider **disabling an account** instead to maintain the history of its records.

To delete an administrator account:

- 1 Select **Administration > Accounts** from the menu.
- 2 Select an account from the list.
- 3 Select **Delete**.
- 4 Confirm that you want to delete this account.

The account is permanently deleted.

Configure General System Settings

You can configure global security settings, MSTP, automatic login for external captive portal, assign vouchers, and limit the IP ranges from which users can log in. You can also activate a contract number from the **General Settings** page.

To configure the general settings:

- 1 From the menu, select **Administration > System**.
- 2 The **General Settings** page opens.

- If there are unassigned switch license vouchers, the Unassigned Switch License Vouchers list displays. [Assign the switch license vouchers to the available devices.](#)



Note

You can change your switch license voucher selection before selecting **Assign**, but not afterward. Assigned switch licenses vouchers cannot be transferred to another device.

- Review any expiring entitlements that display in the **Expiring Entitlements** pane.

General Settings						
Expiring Entitlements						
Entitlement ID	Serial #	Hardware Part Number	Hardware Model	Device Name	Site	Expires On

Figure 165: Expiring Entitlements List

- (Optional) If you enabled location analytics in a site's advanced settings, enter your ExtremeLocation contract number in the **Account Number** field in the **ExtremeLocation** pane.

Extreme Location	
Account Number	<input type="text"/>

Security Policy Settings	
Enable Account Lockout	<input checked="" type="checkbox"/> Number of failed login attempts allowed <input type="text" value="5"/>

Figure 166: Extreme Location Account Number Field

- 6 Edit the **Security Policy Settings** pane, and then select **Save Security Settings**. These enhanced security policy settings are global.

Security Policy Settings

Enable Account Lockout Number of failed login attempts allowed _____

Enable Password Expiry Password Expiry Interval in Days _____

Password Reuse Choose passwords different from previous _____ Password(s)

Password Min Length Force passwords to have at least _____ number of characters

Passwords must contain at least 1 upper case letter

at least 1 lower case letter

at least 1 digit (0 - 9)

at least 1 of the following symbols: !, @, \$, %, -

Login IP Ranges Only allow access to Dashboard from IP addresses in the specified ranges

Two Factor Authentication Enforce two factor authentication for the users

SAVE SECURITY SETTINGS

Figure 167: Security Policy Settings

Enable Account Lockout	Set the number of failed login attempts allowed before a user has to request a password to be reset. Default: 5
Enable Password Expiry	Set the number of days that the password will be valid before it expires and the user is prompted to select a new password. Default: 90
Password Reuse	Limits the number of times a user can reuse previous passwords. The higher the number, the more secure the account is.
Password Min Length	Set the minimum number of characters that a user is forced to enter to have a valid password. A password will not be created unless this minimum is met. Default: 8
Passwords must contain	Set the parameters that a user must follow when creating a password. Your policy can include enforcing at least one upper case letter, one lower case letter, one digit, or one of these symbols: !, @, \$, %, -
Login IP Ranges	Enable this option to allow access to the dashboard only from IP addresses in the specified ranges. Enter the IP address ranges in the text field that displays when this option is selected. Use the format XXX.XX.XX.XXX - XXX.XX.XX.XXX.
Two Factor Authentication	Globally enables two-factor authentication (also known as 2FA) for increased security. Uses the Google Authenticator app to generate a code that must be entered during login, in addition to the account password.

- 7 Edit the remaining fields.

Network Loop Protection

MSTP Enabled

Captive Portal

Select how would you like to handle operating system software attempts to discover captive portals that you are using:

Allow the OS to discover the portal (Use this option unless directed otherwise by TAC)

Hide the presence of the portal from the OS (occasionally necessary for some older operating systems and browsers)

Quietly drop captive portal discovery requests sent by operating system software

This setting only takes effect if you have enabled captive portal authentication on a network.

Miscellaneous

Activate a Contract Number

Figure 168: MSTP, Captive Portal, and Contract Activation

MSTP Enabled	Enable or disable MSTP. This setting applies to the entire network managed from the cloud management. MSTP enablement allows the bundling of multiple VLANs into one spanning tree topology.
Captive Portal	Determine how you would like to handle attempts made by background operating system processes to discover the captive portal, when one is enabled . The user interface displays text to help you decide which option to use. In general, use the Allow the OS to discover the portal option, unless directed to do otherwise by Support or your captive portal provider.
Activate a Contract Number	Select Activate to add a contract number manually.

- 8 Select **Save** in the upper right corner of the screen.
Your changes are saved.

Configure Email Notifications

Email notifications can be enabled or disabled for a variety of notification types, including whether an upgrade is scheduled, a configuration is changed, a site upgrade has started or is completed, an upgrade is canceled, or a device status has changed.

To manage email notifications:

- 1 Select **Administration > Accounts** from the menu.

- In the **e-Mail Notifications** pane, select (enable) or deselect (disable) the notification types.

e-Mail Notifications

Upgrade Scheduled <input checked="" type="checkbox"/>	Site Upgrade Started <input type="checkbox"/>	Site Upgraded <input type="checkbox"/>
Configuration Changed <input type="checkbox"/>	Device Status Changed <input type="checkbox"/>	Upgrade Cancelled <input type="checkbox"/>

Figure 169: Email Notifications Configuration

- Select **Save**.

Assign Switch Licenses

The **Dashboard** displays a notification when there are licenses that have not been assigned to a switch, including 10 Gbps licenses. You can drill down from the dashboard to assign the licenses.

Licenses can only be assigned to switches that do not yet have an associated license. Once a license has been assigned, you cannot transfer the license to a different switch.

To view and assign licenses:

- Log in to **ExtremeCloud**.

The **Dashboard** opens. If there are unassigned licenses, a message displays at the top of the **Dashboard** window.

- To assign the vouchers, click the message "Click **here** to assign them." Alternatively, select **Administration > System**.

The **General Settings** page opens. The **Assign Licenses** pane only displays if there are unassigned licenses.

- From the **Assign Licenses** list, select **Assign** for a switch.

The **Assign License** dialog opens and displays the licenses that are available to assign to the device.

- Select the license check box that you want to assign. You can change your license selection before assigning it, but not afterward. (Assigned switch licenses cannot be transferred to another device.)
- After the license voucher is assigned to the switch, reboot the switch.

17 Troubleshooting

Understanding LED Patterns for AP Registration

Reset a Port

AP Not Connecting With Cloud

The following topics are available for troubleshooting:

- [Understanding LED Patterns for AP Registration](#) on page 229
- [AP Not Connecting With Cloud](#) on page 232
- [Reset a Port](#) on page 230

Understanding LED Patterns for AP Registration

Use this information to understand LED patterns on your APs during registration with ExtremeCloud. To troubleshoot the AP itself, see the device-specific *Installation Guide* for details about the applicable LED patterns.

The following table shows the LED patterns and the associated status for ExtremeWireless APs when they are connected to cloud management.

Table 14: LED Patterns for ExtremeWireless APs Connecting with ExtremeCloud

Radio B/G LED (Left)	Radio A LED (Right)	Status LED	AP Detailed State
Off	Off	Blink green	Initialization: Power-on self test (POST)
	Blink green	Blink green	Initialization: Random delay
		Blink red	Initialization: No Ethernet
	Solid green	Blink green	Initialization: Vulnerable period (not supported)
		Blink red	Reset to factory defaults
Blink green	Off	Blink green or orange	Network discovery: 802.1x authentication
		Blink red	Failed 802.1x authentication
	Blink green	Blink green or orange	Network discovery: DHCP
		Blink red	Default IP address
	Solid green	Blink green or orange	Network discovery: discovery/connect
		Blink red	Discovery failed
<ul style="list-style-type: none"> • Green - Radio On • Off - Radio Off 	<ul style="list-style-type: none"> • Green - Radio On • Off - Radio Off 	Solid green	Connected

The following table shows the LED patterns and the associated status for ExtremeWireless WiNG APs when they are connected to cloud management.

Table 15: LED Patterns for ExtremeWireless WiNG APs Connecting with ExtremeCloud

Task	5 GHz Activity LED (Amber)	2.4 GHz Activity LED (Green)
Unconfigured Radio	On	On
Normal Operation	<ul style="list-style-type: none"> If this radio band is enabled: Blinks at 5-second intervals If this radio band is disabled: Off If there is activity on this band: Blinks at 1 time per second 	<ul style="list-style-type: none"> If this radio band is enabled: Blinks at 5-second intervals If this radio band is disabled: Off If there is activity on this band: Blinks at 1 time per second
Firmware Update	On	Off
Locate AP Mode	LEDs blink in an alternating green, red and amber pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions.	LEDs blink in an alternating green, red and amber pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions.

Reset a Port

If a port fault is transient, the problem should resolve on its own. You can manually reset the port state by disabling and re-enabling the **PoE State** setting.

- 1 Select **Configure > Devices > Switches** from the menu.
- 2 Select a switch from the list.
The **Configure Switch** page opens.
- 3 Select a port name from the **Name** column.

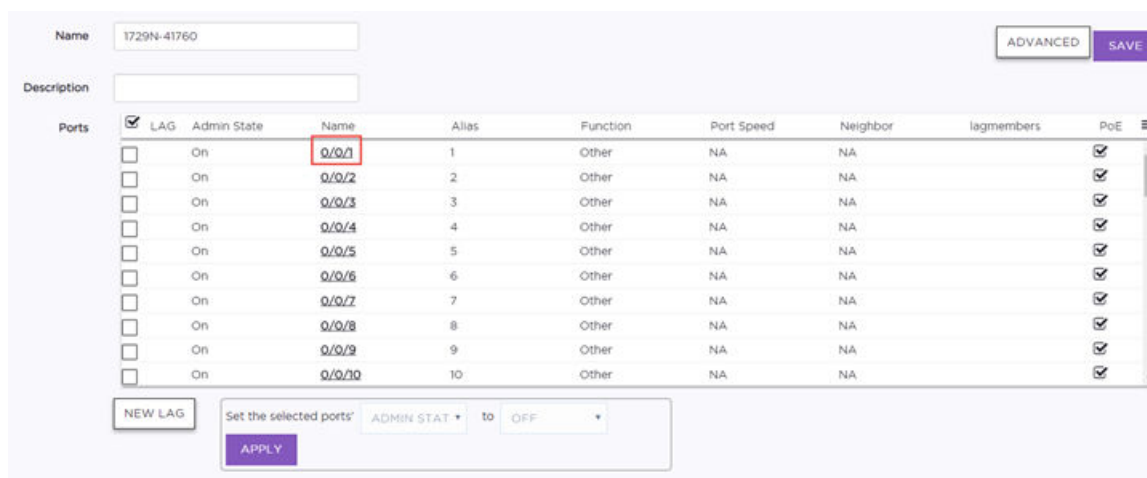


Figure 170: Configure Switch Page

The **Configure Port** page opens.

4 Edit the fields.

The screenshot shows the 'Configure Port' configuration interface. The fields are as follows:

- Name:** 3
- Alias:** 3
- Admin State:** ON
- Function:** OTHER
- PoE Enabled:**
- VLANs:** WING_NAT_TOPOLOGY(2500) (with a plus button to add more)

Name	VLAN IDs	Transmit Tagged	PVID
Default	1	<input type="checkbox"/>	<input checked="" type="radio"/>

Below the table, there are fields for **VLAN Groups** (Name, VLANs) and **Categories** (empty field, plus button).

Figure 171: Configure Port

- Name** Specify a port name.
- Alias** (Optional) Add a user-friendly name as an alias for the port.
- Admin State** Specify whether the port will be enabled or disabled.
- Function** Specify what the switch port will serve as a connection to **APs**, **Interswitch** (uplink), **Host** (such as a printer), **Other**, or **MLAG Interswitch**. If the switch detects an AP using LLDP, the switch will automatically provision the port for that AP. Based on the port role, ExtremeCloud configures VLAN assignments and STP settings (when enabled). You can customize the VLAN settings for **Host** or **Other**. **MLAG Interswitch** is used by MLAG peers to send health-check messages and send MLAG status checkpoint information.
- PoE** Enable or disable Power over Ethernet (PoE) as the power source.
- VLANs** If the function is set to **Host** or **Other**, you can customize the VLAN settings by assigning the port to VLANs, VLAN groups, and categories.
 - VLANs** (Optional) Assign a VLAN from the drop-down list of available VLANs. Select one or more VLANs to assign or delete. A VLAN can be used in more than one VLAN group.

VLAN Groups	(Optional) VLAN Groups are topology groups that contain one or more VLAN IDs. VLAN groups can be assigned to a port or a group of ports, and each port can have more than one VLAN group assigned to it. Each VLAN group is treated as one entity. A VLAN group can also contain VLANs that have more than one VLAN ID assigned to it.
Categories	(Optional) Add or remove from the selected ports. You can create your own category names.
Untagged Traffic	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. Because 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.
Tagged Traffic	The authentication process can indicate a specific role applicable to a user, and the policy definition can dictate how the user's traffic will be presented to the network, including the need to tag traffic to a specific VLAN.
PVID	Specifies that the Port VLAN ID (PVID) will be the default VLAN ID assigned to untagged frames coming in to the port.

- 5 Select **Save**.

AP Not Connecting With Cloud

Condition

ExtremeWireless WiNG AP7632, AP7662, or AP7612 is not connecting with **ExtremeCloud** after upgrading to firmware version 5.9.2.2 and rebooting. I am not using a controller.

Solution

- 1 Verify that the access point is using firmware version 5.9.2.2 or higher. We recommend version 5.9.2.5. For information about how to upgrade your firmware, see the GTAC article: <https://gtacknowledge.extremenetworks.com/articles/Solution/ExtremeCloud-WiNG-Access-Points-not-connecting-to-ezcloudx-com> or see the WiNG AP-specific user documentation.
- 2 Run the Deployment Prerequisite Tool to verify whether there are deployment issues in your environment. Fix the issues and repeat this step until there are no errors in the Prerequisite Tool Verification Summary.
- 3 If the problem persists, open the AP's command line and perform the following steps:
 - 1 Erase the start-up configuration using this command: `erase startup-config`
 - 2 Reboot the AP using this command: `reload`
 - 3 Check the adoption status using this command: `sh adoption status`

The AP should show one of the following messages:

Table 16:

Message	Definition
Discovering adoption mode (controller / cloud / ws-controller) ...	The AP has gone into recovery mode.
Adoption Mode: CLOUD Adopted by: CLOUD	The AP has connected to ExtremeCloud

18 REST API Software Development Kit (SDK)

[Log in to the REST API Server](#)
[Access the Documentation User Interface](#)
[Tools and Methods](#)
[Headers](#)
[Create a Basic REST API Command](#)
[MSP Examples](#)
[Network Management Examples](#)

Welcome to the **ExtremeCloud** Software Development Kit (SDK).

ExtremeCloud uses REST architecture, which is managed using a REST API programmatic interface. This SDK tells you how to access the REST API server, how to access the REST API Documentation GUI, the tools and methods that are supported, and how to use REST API with this product.

More Information

- [Log in to the REST API Server](#) on page 234
- [Access the Documentation User Interface](#) on page 236
- [Tools and Methods](#) on page 237
- [Headers](#) on page 238
- [Create a Basic REST API Command](#) on page 238
- [MSP Examples](#) on page 239
- [Network Management Examples](#) on page 255

Log in to the REST API Server

The fully qualified domain name (FQDN) for the REST API server is: **api.ezcloudx.com**.

You must have administrator credentials to log in to this server. Administrators with read-only privileges can make GET calls using a REST-API consuming program, but only fully privileged accounts can be used to make configuration changes through the REST API. For examples about using the REST API as a network administrator, see [Network Management Examples](#) on page 255.

To perform REST API operations in the MSP space, such as creating MSP partner, you must log in to the API using an account that grants MSP Power Admin privileges. For examples about using the REST API as an MSP Power Administrator, see [MSP Examples](#) on page 239.

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

- 1 From a REST API tool, such as Postman or Advanced REST Client, select the **POST** method and enter the Request URL: `http://api.ezcloudx.com:port/management/v1/oauth2/token`
- 2 Set the header type to **application/JSON**.
- 3 In the **Body** section, enter the request string:

```
{ "grantType": "password", "userId": "example@domain.com", "password": "examplePassword", "scope": "myScope" }
```
- 4 Send the request. You receive an OAUTH2 in a JSON document if the call is successful.

Example: Successful Response

```
{
  "access_token":
  "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJ4YyIsImp0aSI6ImVkyZ2ZmNmJkLWVhZTMtNGEyMClidDQ0LTE1N2QzMjkkNTcyZCJ9.3W_6HiIECAx5ObMcGPRrzzvKGCrvruHJOSfxV-UKU02E",
  "token_type": "Bearer",
  "expires_in": 7200,
  "idle_timeout": 3600,
  "refresh_token":
  "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJ4YyIsImp0aSI6IjUyZjA0ZTJmLTRjZTgtNDBLYi04Njc3LTA0MmI3MTJiM2Q2MCJ9.r7yVcTWF-VrusE0MzMGtY_IldSPPA8gofeJooY2TukQ",
  "twoFactorAuthenticationRequired": false,
  "resetPassword": false,
  "aclTemplate": {
    "id": "88648089-aaab-440a-8c37-598d566fa6af",
    "name": "SE Read Write",
    "aclTemplate": {
      "CreateAdmin": true,
      "CreateMSP": false,
      "CreateMSPEndCustomer": false,
      "CreateMSPPartner": false,
      "CreatePoC": true,
      "CreateSE": false,
      "Delete": true,
      "DeleteAdmin": true,
      "DeleteMSPEndCustomer": false,
      "DeleteMSPPartner": false,
      "DeletePoC": true,
      "DeleteSE": false,
      "DevOps": false,
      "DevopsOnly": false,
      "ERP": false,
      "EndCustomer": false,
      "Extreme TSG": false,
      "ExtremeCloud": false,
      "GTAC": false,
      "GetAdmin": true,
      "GetAllMSP": false,
      "GetAllSE": false,
      "GetMSP": false,

```

```

    "GetMSPPartner": false,
    "GetPoC": true,
    "GetSE": true,
    "GtacCapability": false,
    "MSP": false,
    "MSPPartner": false,
    "ManageERP": false,
    "ManageExtremeCloud": false,
    "ModifyAdmin": true,
    "ModifyMSP": false,
    "ModifyMSPEndCustomer": false,
    "ModifyMSPPartner": false,
    "ModifyPoC": true,
    "ModifySE": false,
    "Read": true,
    "ReadOnlyModifyAdmin": true,
    "ReadWrite": true,
    "ReadWriteCreate": true,
    "SE": true,
    "TSG": false,
    "MspAdmin": false
  },
  "alias": 0,
  "versionTimestamp": 1550471946368000
}
}

```

- To use the token, create an HTTP Authorization Header that includes the authorization token as a Bearer credential. Although each programming tool has its own way to set the header, it is important is that the authorization header is created using the `access_token` from the login response. For the example in the previous step, the Authorization header should look like:

```

authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJ4YyIsImp0aSI6ImVkaWZmNmJkLWVhZTMtNGE5MC1iZDQ0LTE1N2QzMjkkNTcyZCJ9.3W_6HiIECAx5ObMcGPRrzvKGCrvruHJOSfxV-UKUO2E

```

Forward the credentials with each API call.

Access the Documentation User Interface

This topic explains how to access the REST API Documentation GUI for cloud management.

Accessing the Documentation GUI

There are two parts to the REST API documentation:

- An HTML reference user interface, known as the REST API Documentation GUI. It contains a complete list of attributes, elements, and resources. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html
- This SDK guide, which provides information about logging in, tools, methods, headers, and examples.

Logging In to the Documentation GUI

Anyone with ExtremeCloud credentials can log in to the REST API Documentation GUI and view the content.



Note

To submit REST API calls, your REST-API consuming program needs to have logged in using credentials granting at least read permissions for the GET method. Only fully privileged administrator accounts can be used to make configuration changes through the REST API. For more information, see [Log in to the REST API Server](#) on page 234.

More Information

- [Log in to the REST API Server](#) on page 234
- [Tools and Methods](#) on page 237
- [Headers](#) on page 238
- [MSP Examples](#) on page 239
- [Network Management Examples](#) on page 255

Tools and Methods

The REST API is the management interface that allows configuration of the object model state. Configuration changes coming through the GUI or the SDK are written by the REST API. The REST API can be used to manipulate the object model state and retrieve information, such as events and statistics. It can be used to manage tenants, MSP partner, and MSP administration.

You can use any language or library that can submit REST API requests and process JSON. Examples of languages and libraries that have been used to build REST API clients include:

- For Java, the Jersey library provides the reference implementation of JAX-RS, a Java standard for RESTful web services. The implementation includes a client library that can run directly on the JVM.
- For Python, the Requests and JSON libraries facilitate REST API applications.
- For .Net, the core language provides facilities for submitting HTTP requests and .Net libraries include a serializer for JSON.
- For Linux shell, **Wget** and **curl** can execute REST API calls. Linux shell utilities, like **awk** and **grep**, can parse and process JSON.

You can explore the REST API interactively using tools like the Postman plug-in for Chrome.

The API uses a resource manager model. Each resource manager contains data types that have information that can be retrieved and manipulated. In some cases, manipulation or configuration is not allowed and only the GET operation is supported.

The supported CRUD methods (operations) that are available depend on the object. You can find out which methods are supported for each resource manager by looking at the [REST API Documentation GUI](#) and selecting a resource manager.

Generally, the supported methods are:

CRUD Method	Description
GET	Gets information
DELETE	Deletes information
POST	Creates an entry
PUT	Updates an entry

More Information

- [Headers](#) on page 238
- [Create a Basic REST API Command](#) on page 238
- [Access the Documentation User Interface](#) on page 236

Headers

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- `content-type: application/json ;charset=UTF-8`
- `accept: application/json, text/plain, */*`

Any of the following Accept headers are allowed with the Content-Type header request header:

- `accept: application/json`
- `accept-encoding: gzip, deflate, br`
- `accept-language: en-US,en;q=0.8,und;q=0.6`

How you specify the headers depends on the tools you are using:

- **Postman** - Use the tab titled **Headers**, where you can select the header type and specify the value that you want.
- **curl** - Add headers to the request using the '-H' command line option (for example, `-H "Accept:application/json"`).
- **A Programming Language** - The HTTP library you are using likely has a call to set the request headers.

If you get an "unsupported media type" error, it is likely that your program did not specify the content-type header.

Create a Basic REST API Command

Basic CRUD operations (GET, POST, PUT, DELETE) are supported by the REST API.

The basic syntax for an API command is:

```
METHOD HTTP://ipAddress/{v1}\v3/resourceManager/ID/dataType/ID
```

- 1 [Log in to the REST API server as an administrator or MSP Power Admin](#) and get the authorization token.

- 2 Open the [REST API Documentation GUI](#) to find the resource manager and data types that you want to view or configure.
- 3 In your REST API tool (such as Postman), enter your authorization token.
- 4 [Add the headers](#).
- 5 Enter the command (GET, POST, PUT, DELETE) and the URI.

For example:

```
POST HTTP://ipAddress/v1/switches/serialNumber/ports/portNumber
```

- 6 Enter the command body data structure if you are performing a POST or PUT command. (GET and DELETE do not require a body data structure.) The data structure does not need to include all of the attributes and elements that are available to the resource manager, but a minimum set of parameters are required. The minimum set of requirements can be viewed in the [REST API Documentation GUI](#).

For example, the JSON data structure body can follow this input format:

```
{
  "configMethod":
  {
    "attributes":
    {
      "inAttribute": "value1",
      "inAttribute": "value2",
    }
  }
}
```

- 7 Send the call.

The response body is returned with the output attributes if the operation is successful, or an error message is returned if an error is made.

MSP Examples

This section contains a list of examples for MSPs to accomplish tasks using the REST API. MSP Power Admin credentials are required to perform these procedures.



Note

To see network management examples, see [Network Management Examples](#) on page 255

Select a link to open an example:

- [Log in to the REST API Server](#) on page 234
- [Create an MSP Partner](#) on page 240
- [Create an MSP Customer](#) on page 242
- [Move a Customer to a Partner](#) on page 244
- [Move Devices to an MSP Partner](#) on page 247
- [Move Devices to a Customer](#) on page 251

Create an MSP Partner

This procedure outlines how to create an MSP partner account.

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To create a new MSP partner:

- 1 Log in to the REST API server (api.ezcloudx.com) using MSP Power Admin privileges. You must also forward the credentials with each API call.
- 2 Verify that the partner does not already exist by checking your list of current partner using the GET method:

```
GET HTTP://ipAddress/v1/msppartners
```

Example: Response

```
[ {
  "custId" : "MspPartner-id-hcA0LpP5WfsDWslp",
  "id" : null,
  "accountName" : "msp-partner-01",
  "country" : null,
  "timeZone" : null,
  "mspContact" : {
    "custId" : null,
    "id" : null,
    "contactEmail" : "msp-partner-01@test.com",
    "contactName" : "msp-partner-01",
    "contactPhoneNumber" : "1234567890"
  }
} ]
```

- 3 Create the new partner using the POST method:

```
POST HTTP://ipAddress/v1/msppartners
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- content-type: application/json ;charset=UTF-8
- accept: application/json, text/plain, */*

Any of the following Accept headers are allowed with the Content-Type header request header:

- accept: application/json
- accept-encoding: gzip, deflate, br
- accept-language: en-US,en;q=0.8,und;q=0.6

Table 17: Request Attributes

Attribute	Data Type	Description
accountName	String	The user-defined account name of the MSP tenant. Validation: Not null and the length must range from 1 to 64.
entitlements	array of MSPDeviceEntitlementElements	This list contains the devices and the associated entitlement IDs and hardware serial numbers that the MSP partner will manage. The list can be empty during creation and can be updated at any time using the UI or REST API. The device and entitlement IDs must exist and be assigned to the MSP in order for this API call to be able to assign them to a partner.
entitlementId	String	The unique identifier of the entitlement being applied. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
serialNumber	String	The unique identifier of the instance of hardware to which this entitlement applies. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
mspContact	MSPContactElement	The contact details of the MSP partner. Every MSP and MSP partner is required to have a contact name, phone number, and email address.
contactEmail	String	The email address of the MSP for business notifications and for service alerts. Validation: A valid email address.
contactName	String	The contact person for the MSP. Validation: It must be within the range of 1 - 128 characters. Allows alphanumeric and special characters, except semi-colon, colon, and ampersand.
contactPhoneNumber	String	The phone number of the MSP for business notifications and for service alerts. Validation: None
timeZone	String	The timezone of the MSP tenant location. Validation: A valid timezone.
tenants	Array of strings	The list of associated tenants.
userId	String	The first power administrator user ID, it must be an email address and must be unique across all of ExtremeCloud. Validation: The user ID must be a not null and non-empty string (email ID) between 1 and 128 characters long. The string will have 63 characters for the local part (the account/name) and 64 for the domain, the @ sign will be counted extra so that sums to 128. Example: {63}@{64}. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Example: POST Request

```
{
  "accountName": "msp-partner-01",
  "mspContact": {"contactEmail": "msp-partner-01@test.com", "contactName": "msp-partner-01", "contactPhoneNumber": "22222222"},
  "tenants": [],
  "entitlements": [],
```

```

    "userId": "msp-partner-01@test.com"
  }

```

Example: Response

```

{
  "custId" : "Msp-tenantid-Nc5YXfsVtOKdMmsj",
  "id" : null,
  "accountName" : "msp-partner-01",
  "mspContact" : {
    "custId" : null,
    "id" : null,
    "contactEmail" : "msp-partner-01@test.com",
    "contactName" : "msp-partner-01",
    "contactPhoneNumber" : "22222222"
  },
  "userId" : "msp-partner-01@test.com",
  "tenants" : [ ],
  "entitlements" : [ ]
}

```

Example: Error

```

{
  "errors" : [ {
    "errorMessage" : "The phone number entered is invalid. Limits: maximum 15 digits.",
    "resource" : "MSPPartnerElement.mspContact.contactPhoneNumber",
    "errorCode" : 422,
    "messageKey" :
      "exolcore.restapi.elements.MSPContactElement.contactPhoneNumber.isValid",
    "substParams" : [ ],
    "invalidValue" : "222222222222222222"
  } ]
}

```

Create an MSP Customer

This procedure outlines how to create an MSP customer account.

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To create a new MSP customer:

- 1 Log in to the REST API server (api.ezcloudx.com) using MSP Power Admin privileges. You must also forward the credentials with each API call.
- 2 Verify that the customer does not already exist by checking your list of current customers using the GET method:

```
GET HTTP://ipAddress/v1/msptenants
```

Example: Response

```
[ {
  "custId" : "MspEndCustomer-tenantid-hcA0LpP5WfsDWslp",
  "id" : null,
  "accountName" : "msp-customer-01",
  "country" : null,
  "timeZone" : null,
  "mspContact" : {
    "custId" : null,
    "id" : null,
    "contactEmail" : "msp-customer-01@test.com",
    "contactName" : "msp-customer-01",
    "contactPhoneNumber" : "1234567890"
  }
} ]
```

- 3 Create the new customer using the POST method:

```
POST HTTP://ipAddress/v1/msptenants
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- content-type: application/json ;charset=UTF-8
- accept: application/json, text/plain, */*

Any of the following Accept headers are allowed with the Content-Type header request header:

- accept: application/json
- accept-encoding: gzip, deflate, br
- accept-language: en-US,en;q=0.8,und;q=0.6

Table 18: Request Attributes

Attribute	Data Type	Description
accountName	String	The user-defined account name of the MSP tenant. Validation: Not null and the length must range from 1 to 64.
country	Country	The country of MSP tenant. Validation: Valid country codes.
mspContact	MSPContactElement	The contact details of the MSP. Validations: None
contactEmail	String	The email address of the MSP for business notifications and for service alerts. Validation: A valid email address.
contactName	String	The contact person for the MSP. Validation: It must be within the range of 1 - 128 characters. Allows alphanumeric and special characters, except semi-colon, colon, and ampersand.
contactPhoneNumber	String	The phone number of the MSP for business notifications and for service alerts. Validation: None
timeZone	String	The timezone of the MSP tenant location. Validation: A valid timezone.

Example: Request

```
{
  "accountName" : "msp-end-customer-01",
  "country" : "CANADA",
  "timeZone" : "America/New_York",
  "mspContact":{
    "contactEmail" : "msp-end-customer-01@test.com",
    "contactName" : "msp-end-customer-01",
    "contactPhoneNumber" : "1234567890"
  }
}
```

Example: Response

```
{
  "custId": "Msp-tenantid-ZRcCOzB7JX52fezd",
  "id": null,
  "accountName": "msp-end-customer-01",
  "country": "CANADA",
  "timeZone": "America/New_York",
  "mspContact":
  {
    "custId": null,
    "id": null,
    "contactEmail": "msp-end-customer-01@test.com",
    "contactName": "msp-end-customer-01",
    "contactPhoneNumber": "1234567890"
  }
}
```

Example: Error

```
{
  "errorMessage" : "MSP Tenant not found",
  "resource" : "/management/v1/msptenants/Msp-tenantid-swDO5a0sKBCCYAHY",
  "errorCode" : 404,
  "messageKey": "be.resultCode.msp.tenant.notFound",
  "substParams" ; [ ]
} ] ]
}
```

Move a Customer to a Partner

This procedure outlines how to move an unassigned MSP customer account to an MSP partner. This procedure assumes that the customer has already been created. (It is also possible to move a customer from one partner to another partner using a similar procedure.)

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To move an unassigned MSP customer to a partner:

- 1 Log in to the REST API server (api.ezcloudx.com) using MSP Power Admin privileges. You must also forward the credentials with each API call.

- If needed, verify that the customer does not already exist by checking your list of current customers using the GET method:

```
GET HTTP://ipAddress/v1/msptenants/nametoidmap
```

- Get the MSP partner information:

```
GET HTTP://ipAddress/v1/msppartners
```

- Add the list of tenants to the partner document, and then update the document using the PUT method:

```
PUT HTTP://ipAddress/v1/msppartners/{tenantId}
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- `content-type: application/json ;charset=UTF-8`
- `accept: application/json, text/plain, */*`

Any of the following Accept headers are allowed with the Content-Type header request header:

- `accept: application/json`
- `accept-encoding: gzip, deflate, br`
- `accept-language: en-US,en;q=0.8,und;q=0.6`

Table 19: Request Attributes

Attribute	Data Type	Description
tenantId	Path	A non-empty, valid MSP tenant (customer) ID.
accountName	String	The user-defined account name of the MSP tenant. Validation: Not null and the length must range from 1 to 64.
entitlements	Array of MSPDeviceEntitlementElement	A list of device entitlements.
entitlementId	String	The unique identifier of the entitlement being applied. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
serialNumber	String	The unique identifier of the instance of hardware to which this entitlement applies. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
country	Country	The country of MSP tenant. Validation: Valid country codes.
mspContact	MSPContactElement	The contact details of the MSP. Validations: None
contactEmail	String	The email address of the MSP for business notifications and for service alerts. Validation: A valid email address.

Table 19: Request Attributes (continued)

Attribute	Data Type	Description
contactName	String	The contact person for the MSP. Validation: It must be within the range of 1 - 128 characters. Allows alphanumeric and special characters, except semi-colon, colon, and ampersand.
contactPhoneNumber	String	The phone number of the MSP for business notifications and for service alerts. Validation: None
timeZone	String	The timezone of the MSP tenant location. Validation: A valid timezone.
tenants	Array of strings	The list of tenants being assigned to the MSP partner. The tenants must belong to the MSP before they can be assigned to the partner of an MSP. The list of tenants submitted in the response will become the exact list of tenants managed by the MSP partner.
userId	String	The first power administrator user ID, it must be an email address and must be unique across all of ExtremeCloud. Validations: The user ID must be a not null and non-empty string (email ID) between 1 and 128 characters long. The string will have 63 characters for the local part (the account/name) and 64 for the domain, the @ sign will be counted extra so that sums to 128. Example: {63}@{64}. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Example: PUT Request

```
{
  "custId": "MspPartner-tenantid-YLp4lKdq8n6nQNXf",
  "id": null,
  "accountName": "msp-partner-01",
  "mspContact": {"custId": null, "id": null, "contactEmail": "msp-
partner-01@test.com", "contactName": "msp-partner-01", "contactPhoneNumber": "2222222"},
  "userId": null,
  "tenants": ["MspEndCustomer-tenantid-TaLDGFSpg7Vgxt7H"],
  "entitlements": []
}
```

Example: Response

```
{
  "custId" : "Msp-tenantid-Nc5YXfsVtOKdMmsj",
  "id" : null,
  "accountName" : "msp-partner-01",
  "mspContact" : {
    "custId" : null,
    "id" : null,
    "contactEmail" : "msp-partner-01@test.com",
    "contactName" : "msp-partner-01",
    "contactPhoneNumber" : "2222222"
  },
  "userId" : null,
  "tenants" : [ "MspEndCustomer-tenantid-TaLDGFSpg7Vgxt7H" ],
  "entitlements" : [ ]
}
```

Move Devices to an MSP Partner

This procedure outlines how to move devices (access points and switches) from an unassigned state to an MSP partner, or from one MSP partner to another MSP partner.

To move a device to an MSP partner:

- 1 Log in to the REST API server (api.ezcloudx.com) using MSP Power Admin privileges. You must also forward the credentials with each API call.
- 2 Get the list of all APs or switches to determine the serial number and the current state of the device that you want to assign or reassign.

- To get an access point serial number and view its state:

```
GET HTTP://ipAddress/v1/state/aps
```

- To get a switch serial number and view its state:

```
GET HTTP://ipAddress/v1/state/switches
```

- 3 Get the MSP partner **accountName** and **custId**:

```
GET HTTP://ipAddress/v1/msppartners
```

- 4 Create or update the device registration.

Use the POST method to register an unassigned device:

- `POST HTTP://ipAddress/management/v1/deviceregistration/ap/MspPartner-tenantId`
- `POST HTTP://ipAddress/management/v1/deviceregistration/switch/MspPartner-tenantId`

Use the PUT method to move a device from one MSP partner to another MSP partner:

- `PUT HTTP://ipAddress/management/v1/deviceregistration/ap/MspPartner-tenantId`
- `PUT HTTP://ipAddress/managementv1/deviceregistration/switch/MspPartner-tenantId`

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- `content-type: application/json ;charset=UTF-8`
- `accept: application/json, text/plain, */*`

Any of the following Accept headers are allowed with the Content-Type header request header:

- `accept: application/json`
- `accept-encoding: gzip, deflate, br`
- `accept-language: en-US,en;q=0.8,und;q=0.6`

Table 20: Request Attributes: DeviceRegistrationElement

Attribute	Data Type	Description
description	String	Identifies the hardware part number of the device. For access points (APs), the part number provides critical information regarding the regulatory domain the AP is to operate in and provides a way to infer the number of radios in the AP and their capabilities. "WS-AP3935i-ROW" is an example of a valid description. Valid character set : Alphanumeric and special characters, except semi-colon, colon, and ampersand.
deviceName	String	A user-defined, human friendly name for the device. The attribute defaults to the serial number but, unlike serialNumber, an administrator with write privileges can change this attribute at any time. Validations : A not null and non-empty string having maximum of 255 characters. Valid character set : Alphanumeric and special characters, except semi-colon, colon, and ampersand.
lan1Mac	String	The MAC layer address of one of the device's physical wired interfaces. This is usually the interface through which the device will be managed. In the case of Extreme Networks access points, one of the MAC address of one of the wired interfaces of the AP is used. The MAC address is optional but useful. The MAC address is a sequence of 12 ASCII-encode hexadecimal digits without separators. Validations : A not null and non-empty hexadecimal string with no separators. Valid character set : Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Table 20: Request Attributes: DeviceRegistrationElement (continued)

Attribute	Data Type	Description
lan2Mac	String	The MAC address of the second wired physical wired interface, if it has one. This MAC address is optional, but useful to know. The MAC address is a sequence of 12 ASCII-encoded hexadecimal digits without separators. "a1b2c3d41621" is an example of a correctly formatted MAC address. Validations: A not null and non-empty hexadecimal string with no separators. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
manufacturingLot	String	(Optional) The manufacturer's lot number. This can be helpful in the event that the device belongs to a batch that is known to be faulty. In the case of Extreme Network access points, the lot number is embedded in the device serial number. Valid character set: Alphanumeric and special characters except semi-colon, colon, and ampersand.
serialNumber	String	The globally unique serial number of the device being registered. The serial number is represented as a string. The actual length and format of the string depends on the type of device being registered. This is the only attribute of the device that must not be null. Senao refers to this field as 'Prog#' on the label. "1507Y-1000100000" is an example of a valid serial number. Validations: A not null and non-empty string having exactly 16 characters for APs. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Table 20: Request Attributes: DeviceRegistrationElement (continued)

Attribute	Data Type	Description
wan1Mac	String	(Optional) The MAC layer address of one of an access point's physical wireless interfaces. The MAC address is a sequence of 12 ASCII-encode hexadecimal digits without separators. "a1b2c3d41621" is an example of a correctly formatted MAC address. Validations: A not null and non-empty hexadecimal string with no separators. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
wan2Mac	String	(Optional) The MAC layer address of one of an access point's physical wireless interfaces. Physical switches will not have these interfaces. The MAC address is a sequence of 12 ASCII-encode hexadecimal digits without separators. "a1b2c3d41621" is an example of a correctly formatted MAC address. Validations: A not null and non-empty hexadecimal string with no separators. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Example: PUT Request

```
{
  "userid": "msp-01@test.com",
  "siteRegistration": {
    "siteName": "",
    "country": null,
    "timeZone": null,
    "latitude": null,
    "longitude": null
  },
  "devices": [
    {
      "serialNumber": "0000Y-0000000000",
      "deviceName": "0000Y-0000000000",
      "description": "AP3935i-FCC",
      "lan1Mac": null,
      "lan2Mac": null,
      "wan1Mac": null,
      "wan2Mac": null,
      "manufacturingLot": ""
    }
  ]
}
```

Example: Response

```
{
  "userid": "msp-01@test.com",
  "siteRegistration": {
    "siteName": "",
    "country": null,
    "timeZone": null,
    "latitude": null,
    "longitude": null
  },
  "devices": [
    {
      "serialNumber": "0000Y-0000000000",
      "deviceName": "0000Y-0000000000",
      "description": "AP3935i-FCC",
      "lan1Mac": null,
      "lan2Mac": null,
      "wan1Mac": null,
      "wan2Mac": null,
      "manufacturingLot": ""
    }
  ]
}
```

```
"wan1Mac":null,
"wan2Mac":null,
"manufacturingLot":""}}}
```

Move Devices to a Customer

This procedure outlines how to move devices (access points and switches) from an unassigned state to an MSP partner, or from one MSP partner to another MSP partner.

To move a device to an MSP partner:

- 1 Log in to the REST API server (api.ezcloudx.com) using MSP Power Admin privileges. You must also forward the credentials with each API call.
- 2 Get the list of all APs or switches to determine the serial number and the current state of the device that you want to assign or reassign.

- To get an access point serial number and view its state:

```
GET HTTP://ipAddress/v1/state/aps
```

- To get a switch serial number and view its state:

```
GET HTTP://ipAddress/v1/state/switches
```

- 3 Get the customer **accountName** and **custId**:

```
GET HTTP://ipAddress/v1/customers
```

- 4 Create or update the device registration.

Use the POST method to register an unassigned device:

- POST `HTTP://ipAddress/management/v1/deviceregistration/ap/MspEndCustomer-tenantId`
- POST `HTTP://ipAddress/management/v1/deviceregistration/switch/MspEndCustomer-tenantId`

Use the PUT method to move a device from one customer to another customer:

- PUT `HTTP://ipAddress/management/v1/deviceregistration/ap/MspEndCustomer-tenantId`
- PUT `HTTP://ipAddress/managementv1/deviceregistration/switch/MspEndCustomer-tenantId`

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- `content-type: application/json ;charset=UTF-8`
- `accept: application/json, text/plain, */*`

Any of the following Accept headers are allowed with the Content-Type header request header:

- `accept: application/json`
- `accept-encoding: gzip, deflate, br`
- `accept-language: en-US,en;q=0.8,und;q=0.6`

Table 21: Request Attributes: DeviceRegistrationElement

Attribute	Data Type	Description
description	String	Identifies the hardware part number of the device. For access points (APs), the part number provides critical information regarding the regulatory domain the AP is to operate in and provides a way to infer the number of radios in the AP and their capabilities. "WS-AP3935i-ROW" is an example of a valid description. Valid character set : Alphanumeric and special characters, except semi-colon, colon, and ampersand.
deviceName	String	A user-defined, human friendly name for the device. The attribute defaults to the serial number but, unlike serialNumber, an administrator with write privileges can change this attribute at any time. Validations : A not null and non-empty string having maximum of 255 characters. Valid character set : Alphanumeric and special characters, except semi-colon, colon, and ampersand.
lan1Mac	String	The MAC layer address of one of the device's physical wired interfaces. This is usually the interface through which the device will be managed. In the case of Extreme Networks access points, one of the MAC address of one of the wired interfaces of the AP is used. The MAC address is optional but useful. The MAC address is a sequence of 12 ASCII-encode hexadecimal digits without separators. Validations : A not null and non-empty hexadecimal string with no separators. Valid character set : Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Table 21: Request Attributes: DeviceRegistrationElement (continued)

Attribute	Data Type	Description
lan2Mac	String	The MAC address of the second wired physical wired interface, if it has one. This MAC address is optional, but useful to know. The MAC address is a sequence of 12 ASCII-encoded hexadecimal digits without separators. "a1b2c3d41621" is an example of a correctly formatted MAC address. Validations: A not null and non-empty hexadecimal string with no separators. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
manufacturingLot	String	(Optional) The manufacturer's lot number. This can be helpful in the event that the device belongs to a batch that is known to be faulty. In the case of Extreme Network access points, the lot number is embedded in the device serial number. Valid character set: Alphanumeric and special characters except semi-colon, colon, and ampersand.
serialNumber	String	The globally unique serial number of the device being registered. The serial number is represented as a string. The actual length and format of the string depends on the type of device being registered. This is the only attribute of the device that must not be null. Senao refers to this field as 'Prog#' on the label. "1507Y-1000100000" is an example of a valid serial number. Validations: A not null and non-empty string having exactly 16 characters for APs. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Table 21: Request Attributes: DeviceRegistrationElement (continued)

Attribute	Data Type	Description
wan1Mac	String	(Optional) The MAC layer address of one of an access point's physical wireless interfaces. The MAC address is a sequence of 12 ASCII-encode hexadecimal digits without separators. "a1b2c3d41621" is an example of a correctly formatted MAC address. Validations: A not null and non-empty hexadecimal string with no separators. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
wan2Mac	String	(Optional) The MAC layer address of one of an access point's physical wireless interfaces. Physical switches will not have these interfaces. The MAC address is a sequence of 12 ASCII-encode hexadecimal digits without separators. "a1b2c3d41621" is an example of a correctly formatted MAC address. Validations: A not null and non-empty hexadecimal string with no separators. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Example: PUT Request

```
{ "userid": "msp-01@test.com",
  "siteRegistration": { "siteName": "",
    "country": null,
    "timeZone": null,
    "latitude": null,
    "longitude": null },
  "devices": [ { "serialNumber": "0000N-00000",
    "deviceName": "0000N-00000",
    "description": "X440G2-12t-10G4",
    "lan1Mac": null,
    "lan2Mac": null,
    "wan1Mac": null,
    "wan2Mac": null, "manufacturingLot": "" } ] }
```

Example: Response

```
{ "userid": "msp-01@test.com",
  "siteRegistration": { "siteName": "",
    "country": null,
    "timeZone": null,
    "latitude": null,
    "longitude": null },
  "devices": [ { "serialNumber": "0000N-00000",
    "deviceName": "0000N-00000",
```

```
"description": "X440G2-12t-10G4",
"lan1Mac": null,
"lan2Mac": null,
"wan1Mac": null,
"wan2Mac": null, "manufacturingLot": "" }}}
```

Network Management Examples

This section contains a list of examples of using the REST API to manage your network. Credentials granting write privileges as well as read privileges are required to change the configuration.



Note

To see MSP examples, see [MSP Examples](#) on page 239

Select a link to open an example:

- [Create a Role and Assign it to a Site](#) on page 255
- [Create a Network and Assign it to a Site](#) on page 263
- [Assign Port Functions](#) on page 274
- [Update an Access Point's Configuration](#) on page 279
- [Change a Preshared Key](#) on page 285

Create a Role and Assign it to a Site

This procedure outlines how to create a new role and assign it to a site. A role must be assigned to a site to be usable.



Note

The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To create a role and assign it to a site:

- 1 Log in to the REST API server (api.ezcloudx.com) using administrator credentials. You must also forward the credentials with each API call. For an example of how to log in, see [Log in to the REST API Server](#) on page 234.
- 2 Verify that the role does not already exist by checking the list of current roles using the GET method:

```
GET HTTP://ipAddress/v3/roles
```

- 3 Create the new role instance using the POST method:

```
POST HTTP://ipAddress/v3/roles
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- `content-type: application/json ;charset=UTF-8`

- `accept: application/json, text/plain, */*`

Any of the following Accept headers are allowed with the Content-Type header request header:

- `accept: application/json`
- `accept-encoding: gzip, deflate, br`
- `accept-language: en-US,en;q=0.8,und;q=0.6`

Table 22: Request Attributes

Attribute	Data Type	Description
cpAddApNameAndSerial	Boolean	A flag to indicate if the AP serial number and name should be added as a parameter for external captive portal (ECP) authentication.
cpAddBssid	Boolean	A flag to indicate if the access point's BSSIDs should be added as a parameter for ECP authentication.
cpAddIpAndPort	Boolean	A flag to indicate if IP address and port should be added as a parameter for ECP authentication.
cpAddMac	Boolean	A flag to indicate if the client's MAC should be added as a parameter for ECP authentication.
cpAddRole	Boolean	A flag to indicate if the current role assigned to the client should be added as a parameter for ECP authentication.
cpAddSign	Boolean	A flag to indicate if the AWS Signature should be added as a parameter for ECP authentication.
cpAddSsid	Boolean	A flag to indicate if SSID should be added as a parameter for ECP authentication.
cpAddTime	Boolean	A flag to indicate if time should be added as a parameter for ECP authentication.
cpAddVlan	Boolean	A flag to indicate if the current VLAN assigned to the client should be added as a parameter for ECP authentication.
cpAddVnsName	Boolean	A flag to indicate if Virtual Network segment name should be added as a parameter for ECP authentication.
cpDefaultRedirectUrl	String	The redirection URL to which the wireless device user will be directed to after authentication.
cpHttp	Boolean	A flag to indicate if HTTP should be used.
cpIdentity	String	The identity used by the ECP and AP redirecting station to identify each other. Validations: A not null and non-empty string, having maximum of 255 characters, if any of the filter rule has an action as 'FILTERACTION_REDIRECT'.
cpRedirect	String	The URL of the captive portal login page.
cpRedirectUrlSelect	RedirUrlSelect	The post-authentication URL selection.

Table 22: Request Attributes (continued)

Attribute	Data Type	Description
cpSharedKey	String	The shared secret (used with identity to sign and encrypt the redirection URL). It is a password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external web server. Validations: A not null and non-empty string, between 8 and 64 characters, if any of the filter rules has an action as 'FILTERACTION_REDIRECT'.
defaultAction	PolicyAccessControlAction	The default access control action to be applied when there are no policy rules or none of the rules match the frame. Validations: A not null and valid PolicyAccessControlAction value as a string.
defaultCos	String	The class of service (CoS) to assign to a matching frame if the role has no rules, or none of the rules match the frame or if none of the rules that match the frame assign a CoS to the frame. Set this to null to indicate that no CoS will be applied to the frame. In that case the frame's QoS fields will not be remarked and the traffic will not be rate limited in either direction. Validations: A valid UUID of a CoS.
features	Array of strings	A list of supported features.
filters	Array of PolicyRuleElement filters	A list of rule filters associated with the role. More information about filters is available at: http://documentation.extremenetworks.com/extremecloud/rest_api/index.html
name	String	The role name that is unique across the customer sites. Validations: A not null and non-empty string, between 1 to 255 characters. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
topology	String	If defaultAction == containToVlan, the topology must reference a defined topology. If defaultAction has any other value, the topology should be null and in any case it will be ignored/discarded. Validations: A valid UUID of a topology.

- 4 Assign the role to an existing site.

```
PUT HTTP://ipAddress/v3/management/sites/siteID
```

Example: POST Request - Create a Role

```
{
  "custId": "1-25R001C",
  "id": "26820c30-a870-11e7-8fd1-a34beb33e832",
  "name": "Role_1",
  "filters": null,
  "l2Filters": [{
    "name": "filter-1",
    "intoNetwork": "destAddr",
    "outFromNetwork": "sourceAddr",
    "action": "FILTERACTION_ALLOW",
    "topologyId": null,
  }
]
```

```

    "cosId":null,
    "userDefinedEthertype":2048,
    "macAddrType":"user_defined",
    "macAddress":"11:22:33:44:55:66",
    "ethertype":"ipv4","userPriority":"notApplicable"
  ]],
  "l3Filters":[],
  "l7Filters":[],
  "defaultAction":"deny",
  "topology":null,
  "defaultCos":"86500336-ed48-11e5-9ce9-5e5517507c66",
  "cpRedirect":null,
  "features":["APP-CONTROL","CP-AT-AP","CP-AT-AP-PRONTO","IPV6","WIRED-PORTS"],
  "cpIdentity":"","
  "cpSharedKey":"","
  "cpDefaultRedirectUrl":null,
  "cpRedirectUrlSelect":"URLTARGET",
  "cpHttp":false,
  "cpAddIpAndPort":true,
  "cpAddApNameAndSerial":true,
  "cpAddBssid":true,
  "cpAddVnsName":true,
  "cpAddSsid":true,
  "cpAddMac":true,
  "cpAddRole":true,
  "cpAddVlan":true,
  "cpAddTime":true,
  "cpAddSign":true
}

```

Example: Response - Create a Role

```

{
  "custId" : "1-25R001C",
  "id" : "26820c30-a870-11e7-8fd1-a34beb33e832",
  "name" : "Role_1",
  "filters" : null,
  "l2Filters" : [ {
    "custId" : null,
    "id" : null,
    "name" : "filter-1",
    "intoNetwork" : "destAddr",
    "outFromNetwork" : "sourceAddr",
    "action" : "FILTERACTION_ALLOW",
    "topologyId" : null,
    "cosId" : null,
    "userDefinedEthertype" : 2048,
    "macAddrType" : "user_defined",
    "macAddress" : "11:22:33:44:55:66",
    "ethertype" : "ipv4",
    "userPriority" : "notApplicable"
  } ],
  "l3Filters" : [ ],
  "l7Filters" : [ ],
  "defaultAction" : "deny",
  "topology" : null,
  "defaultCos" : "86500336-ed48-11e5-9ce9-5e5517507c66",
  "cpRedirect" : null,
  "features" : [ "APP-CONTROL", "CP-AT-AP", "CP-AT-AP-PRONTO", "IPV6", "WIRED-PORTS" ],
  "cpIdentity" : null,
  "cpSharedKey" : null,
  "cpDefaultRedirectUrl" : null,
  "cpRedirectUrlSelect" : "URLTARGET",

```

```

"cpHttp" : false,
"cpAddIpAndPort" : true,
"cpAddApNameAndSerial" : true,
"cpAddBssid" : true,
"cpAddVnsName" : true,
"cpAddSsid" : true,
"cpAddMac" : true,
"cpAddRole" : true,
"cpAddVlan" : true,
"cpAddTime" : true,
"cpAddSign" : true
}

```

Example: PUT Request - Update a Site

```

{
  "custId":"1-25R001C",
  "id":"0c891450-a85b-11e7-8fd1-a34beb33e832",
  "siteName":"Default",
  "country":"UNITED_STATES",
  "timezone":"America/New_York",
  "scheduleUpgradeInfo":{
    "custId":null,
    "id":null,
    "preferredDayOfWeek":null,
    "preferredWeek":null,
    "preferredTime":{
      "custId":null,
      "id":null,
      "hour":0,
      "minute":0
    }
  },
  "siteManagerName":null,
  "siteManagerEmail":null,
  "contact":null,
  "smartRFPolicy":{
    "custId":null,
    "id":null,
    "txMinimumPower5":3,
    "txMaximumPower5":16,
    "txMinimumPower24":3,
    "txMaximumPower24":16,
    "acsChannelSelection5":"CHPLAN_ALLBYCOUNTRY",
    "acsChannelSelectionList5":
["157+1/40","100/40","140+1/40","132+1/40","140/40","108/40","36/40","165/40","100+1/40","
132/40","149+1/40","157/40","44/40","149/40","60+1/40","108+1/40","116+1/40","52/40","124/
40","124+1/40","44+1/40","52+1/40","36+1/40","116/40","60/40"],
    "acsChannelSelection24":"CHPLAN_AUTO",
    "acsChannelSelectionList24":["11","1","6"],
    "dot11nChannelWidth5":"Ch1Width_40MHz",
    "dot11nChannelWidth24":"Ch1Width_20MHz",
    "rfSensitivity":"medium",
    "ocsClientAware24":0,
    "ocsClientAware5":0,
    "ocsVoiceAware24":"dynamic",
    "ocsVoiceAware5":"dynamic",
    "interferenceRecovery":true,
    "coverageHoleRecovery":true,
    "neighborRecovery":true,
    "minInterferenceChannelSwitch5":20,
    "minInterferenceChannelSwitch24":20,
    "minSnrThreshold5":20,

```

```

"minSnrThreshold24":20,
"runOcsScanOncePerDay":false,
"dcsNoiseInterferenceThreshold5":-80,
"dcsChannelOccupanyThreshold5":100,
"dcsUpdatePeriod5":5,
"dcsNoiseInterferenceThreshold24":-80,
"dcsChannelOccupanyThreshold24":100,
"dcsUpdatePeriod24":5,"interferenceWaitTime24":10
},
"managementPolicy":{
  "custId":null,
  "id":null,
  "name":null,"adminPassword":null,
  "enableTraps":false,
  "snmpTrapReceivers":[],
  "snmpUSMs":[]
},
"deviceGroups":[{"
  "custId":null,
  "id":"0c891450-a85b-11e7-8fd1-a34beb33e832",
  "groupName":null,
  "loadBalanceBandPreferenceEnabled":false,
  "roleIds":["148c4042-efb0-11e5-9ce9-5e5517507c66","91f27cd0-8fcb-11e5-8994-
feff819cdc9f","0c1c48c0-a85b-11e7-8fd1-a34beb33e832","26820c30-a870-11e7-8fd1-
a34beb33e832"],
  "apSerialNumbers":["1549Y-1019600000"],
  "switchSerialNumbers":["1551N-40607"],
  "topologyIDs":["87b7f72c-8fcb-11e5-8994-feff819cdc9f"],
  "serviceIDs":[],
  "backboneTopologyIDs":[],
  "radioAssignment":[{"
    "serviceId":"0c602f90-a85b-11e7-8fd1-a34beb33e832",
    "radioBand":"Band5"
  }, {
    "serviceId":"0c602f90-a85b-11e7-8fd1-a34beb33e832",
    "radioBand":"Band24"
  }, {
    "serviceId":"f0e17380-a870-11e7-8fd1-a34beb33e832",
    "radioBand":"Band5"
  }, {
    "serviceId":"f0e17380-a870-11e7-8fd1-a34beb33e832",
    "radioBand":"Band24"
  } ],
  "wiredInterfaceAssignment":[],
  "enableDpi":true,"minimumBaseRate2_4":6,
  "minimumBaseRate5":6,
  "aggregateMpdu2_4":true,
  "aggregateMpdu5":true,
  "stbcEnabled2_4":false,
  "stbcEnabled5":false,
  "txbfEnabled2_4":"disabled",
  "txbfEnabled5":"muMimo",
  "dnsServers":["0.0.0.0"]
} ],
"treeNode":{
  "custId":null,
  "id":null,"country":null,
  "region":null,
  "campus":null,
  "city":null,
  "mapCoordinates":null
},
"snmpConfig":{
  "custId":null,

```

```

    "id":null,
    "snmpVersion":"DISABLED",
    "v2Communities":{},
    "v3Users":[],
    "notifications":[]
  },
  "syslogConfiguration":{
    "custId":null,
    "id":null,
    "enabled":false,
    "logging":"INFO",
    "syslogConfig":{"":514},
    "logGuestTraffic":false
  },
  "siteType":"IDENTIFI",
  "features":["APP-CONTROL","CP-AT-AP","CP-AT-AP-PRONTO","IPV6","WIRED-PORTS"],"floorIds":
[]
}

```

Example: Response - Update a Site

```

{
  "custId" : "1-25ROO1C",
  "id" : "0c891450-a85b-11e7-8fd1-a34beb33e832",
  "siteName" : "Default",
  "country" : "UNITED_STATES",
  "timezone" : "America/New_York",
  "scheduleUpgradeInfo" : {
    "custId" : null,
    "id" : null,
    "preferredDayOfWeek" : null,
    "preferredWeek" : null,
    "preferredTime" : {
      "custId" : null,
      "id" : null,
      "hour" : 0,
      "minute" : 0
    }
  },
  "siteManagerName" : null,
  "siteManagerEmail" : null,
  "contact" : null,
  "smartRFPolicy" : {
    "custId" : null,
    "id" : null,
    "txMinimumPower5" : 3,
    "txMaximumPower5" : 16,
    "txMinimumPower24" : 3,
    "txMaximumPower24" : 16,
    "acsChannelSelection5" : "CHPLAN_ALLBYCOUNTRY",
    "acsChannelSelectionList5" : [ "157+1/40", "100/40", "140+1/40", "132+1/40",
"140/40", "108/40", "36/40", "165/40", "100+1/40", "132/40", "149+1/40", "157/40",
"44/40", "149/40", "60+1/40", "108+1/40", "116+1/40", "52/40", "124/40", "124+1/40",
"44+1/40", "52+1/40", "36+1/40", "116/40", "60/40" ],
    "acsChannelSelection24" : "CHPLAN_AUTO",
    "acsChannelSelectionList24" : [ "11", "1", "6" ],
    "dot11nChannelWidth5" : "Ch1Width_40MHz",
    "dot11nChannelWidth24" : "Ch1Width_20MHz",
    "rfSensitivity" : "medium",
    "ocsClientAware24" : 0,
    "ocsClientAware5" : 0,
    "ocsVoiceAware24" : "dynamic",
    "ocsVoiceAware5" : "dynamic",
    "interferenceRecovery" : true,

```

```

    "coverageHoleRecovery" : true,
    "neighborRecovery" : true,
    "minInterferenceChannelSwitch5" : 20,
    "minInterferenceChannelSwitch24" : 20,
    "minSnrThreshold5" : 20,
    "minSnrThreshold24" : 20,
    "runOcsScanOncePerDay" : false,
    "dcsNoiseInterferenceThreshold5" : -80,
    "dcsChannelOccupanyThreshold5" : 100,
    "dcsUpdatePeriod5" : 5,
    "dcsNoiseInterferenceThreshold24" : -80,
    "dcsChannelOccupanyThreshold24" : 100,
    "dcsUpdatePeriod24" : 5,
    "interferenceWaitTime24" : 10
  },
  "managementPolicy" : {
    "custId" : null,
    "id" : null,
    "name" : null,
    "adminPassword" : null,
    "enableTraps" : false,
    "snmpTrapReceivers" : [ ],
    "snmpUSMs" : [ ]
  },
  "deviceGroups" : [ {
    "custId" : null,
    "id" : "0c891450-a85b-11e7-8fd1-a34beb33e832",
    "groupName" : null,
    "loadBalanceBandPreferenceEnabled" : false,
    "roleIDs" : [ "148c4042-efb0-11e5-9ce9-5e5517507c66", "91f27cd0-8fcb-11e5-8994-feff819cdc9f", "0c1c48c0-a85b-11e7-8fd1-a34beb33e832", "26820c30-a870-11e7-8fd1-a34beb33e832" ],
    "apSerialNumbers" : [ "1549Y-1019600000" ],
    "switchSerialNumbers" : [ "1551N-40607" ],
    "topologyIDs" : [ "87b7f72c-8fcb-11e5-8994-feff819cdc9f" ],
    "serviceIDs" : [ "0c602f90-a85b-11e7-8fd1-a34beb33e832" ],
    "backboneTopologyIDs" : [ ],
    "radioAssignment" : [ {
      "custId" : null,
      "id" : null,
      "serviceId" : "0c602f90-a85b-11e7-8fd1-a34beb33e832",
      "radioBand" : "Band5"
    }, {
      "custId" : null,
      "id" : null,
      "serviceId" : "0c602f90-a85b-11e7-8fd1-a34beb33e832",
      "radioBand" : "Band24"
    } ],
    "wiredInterfaceAssignment" : [ ],
    "enableDpi" : true,
    "minimumBaseRate2_4" : 6,
    "minimumBaseRate5" : 6,
    "aggregateMpdu2_4" : true,
    "aggregateMpdu5" : true,
    "stbcEnabled2_4" : false,
    "stbcEnabled5" : false,
    "txbfEnabled2_4" : "disabled",
    "txbfEnabled5" : "muMimo",
    "dnsServers" : [ "0.0.0.0" ]
  } ],
  "treeNode" : {
    "custId" : null,
    "id" : null,
    "country" : null,

```

```

    "region" : null,
    "campus" : null,
    "city" : null,
    "mapCoordinates" : null
  },
  "snmpConfig" : {
    "custId" : null,
    "id" : null,
    "snmpVersion" : "DISABLED",
    "v2Communities" : { },
    "v3Users" : [ ],
    "notifications" : [ ]
  },
  "syslogConfiguration" : {
    "custId" : null,
    "id" : null,
    "enabled" : false,
    "logging" : "INFO",
    "syslogConfig" : { },
    "logGuestTraffic" : false
  },
  "siteType" : "IDENTIFI",
  "features" : [ "APP-CONTROL", "CP-AT-AP", "CP-AT-AP-PRONTO", "IPV6", "WIRED-PORTS" ],
  "floorIds" : [ ]
}

```

Create a Network and Assign it to a Site

This procedure outlines how to create a new network and assign it to a site. A network must be assigned to a site to be usable.

We recommend configuring the default settings or creating new services (SSIDs).

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To create a network and assign it to a site:

- 1 Log in to the REST API server (api.ezcloudx.com) using administrator credentials. You must also forward the credentials with each API call. For an example of how to log in, see [Log in to the REST API Server](#) on page 234.
- 2 Create the new network service using the POST method. The network data type is Service Element, which is comprised of a set of one or more topologies that also include a network authentication, an authorization strategy, an edge privacy (encryption) policy (open, WPAv2), a default access control policy. It can be enabled or disabled manually or (eventually) on a schedule. Some attributes are required, such as serviceName.

```
POST HTTP://{ipAddress}/v1/services
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- `content-type: application/json ;charset=UTF-8`
- `accept: application/json, text/plain, /*/*`

Any of the following Accept headers are allowed with the Content-Type header request header:

- `accept: application/json`
- `accept-encoding: gzip, deflate, br`
- `accept-language: en-US,en;q=0.8,und;q=0.6`

Table 23: Request Attributes

Attribute	Data Type	Description
WpaEnterpriseElement	WpaEnterpriseElement	A class that contains a bag of settings specific to the specific privacy implementation used by this service. Privacy is null if the user has selected the Privacy = None option. For the prototype, none ("no privacy") and WPAv2-PSK are supported.
WpaPskElement	WpaPskElement	A class that contains a bag of settings specific to the specific privacy implementation used by this service. Privacy is null if the user has selected the Privacy = None option. For the prototype, none ("no privacy") and WPAv2-PSK are supported.
aaaPolicy	String	Configures AAAPolicy for this service.
admissionControlBackgroundTraffic	Boolean	Select to enable Global Admission Control for Background Traffic. This feature is only available if admission control is enabled for Background. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands.
admissionControlBestEffort	Boolean	Select to enable Global Admission Control for Best Effort. If the client does not support admission control for the access category that requires admission control, the traffic category will be downgraded to a lower access category that does not have mandatory admission control. For example, if admission control is required for video, and client does not support admission control for video, traffic will be downgraded to Best Effort (BE).
admissionControlVideo	Boolean	Select to provide distinct thresholds for VI (video). This feature is only available if admission control is enabled for voice. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands.
admissionControlVoice	Boolean	Select to enable Admission Control for Voice. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands.
airtimeFairness	Boolean	Select to enable airtime fairness.

Table 23: Request Attributes (continued)

Attribute	Data Type	Description
authenticatedUserDefaultRoleID	String	(Required Attribute) Default role Id for authenticated user. Validations: A not null value and a valid UUID.
azaraCos	String	The Azara inbound and outbound ratelimiter profile.
bridgingMode	BridgingMode	Configures how packets to/from this WLAN are bridged. Packets are bridged between WLAN and local Ethernet ports. Packets are tunneled to other devices, typically wireless controllers (local/tunnel).
captivePortalId	String	The captive portal UUID.
classification	SSIDClassification	All traffic on this WLAN is treated as WMM (DSCP or 802.1p to different queues); voice, video, normal priority (BestEffort), or low priority traffic (Background).
clientLoadBalancing	Boolean	A flag to enable client traffic load balancing.
clientToClientCommunication	Boolean	A flag to enable client-to-client communication in a WLAN.
defaultCoS	String	The default class of service to assign to frames that are not assigned a CoS by the role assigned to the station generating the traffic. Set this to null to leave unchanged the CoS of frames not assigned a CoS explicitly by the role of the station generating traffic. Default: null Implementation details: This can just be a string containing the name of a defined CoS. Validations: A valid UUID of CoS.
defaultTopology	String	The topology (VLAN) that traffic should be placed on by default when the role assigned to the station generating the traffic does not specify the VLAN on which to forward traffic. This can be null, but it is usually easiest to assign a topology to the service than to use roles just to allow or deny specific types of traffic. Default: null Implementation detail: This can just be a string containing the name of a defined topology. Validations: A valid UUID of a topology.
enableCaptivePortal	Boolean	A flag to enable captive portal.
enabled11kSupport	Boolean	Enable support for 802.11k radio management. Setting this attribute to true enables the feature and setting to false disables the feature. When the feature is enabled, then support for transmitting the Quiet IE and for the 11k Beacon report are also enabled. Disabling 11k support disables the use of the quiet IE and the 11k Beacon report. Default: false (disabled)
enabledSchedule	ServiceWeeklyScheduleElement	The time during which this service is enabled. It is the same time range for each site at which the service is available. Note that most UI's might want to offer simple checklists for time ranges to support (Always, Weekdays only, Office hours only, Never, etc.) and only expose an exact representation of the following data structure as an advanced option.
features	Array of strings	A list of supported features.

Table 23: Request Attributes (continued)

Attribute	Data Type	Description
flexibleClientAccess	Boolean	Enabling this feature causes an access point (AP) to take steps to ensure that fast clients with content to send will get as much airtime as slow clients. When this is feature is turned off, the AP treats all clients equally and processes packet forwarding requests on a First-Come-First-Serve basis. Default: disable
mbaAuthorization	Boolean	Select to enable MBA authorization.
mbatimeoutRoleId	String	The MAC-based authentication timeout role ID. Validations: A valid UUID of a role.
mgmtFrameProtection	MgmtFrameProtection	The management frame protection to use (disabled/enabled/required).
openDNSDeviceId	String	Content filtering using open DNS.
policyOnRadiusTimeout	String	A role to apply if the rejectonradiustimeout = false and the RADIUS request times out.
postAuthenticatedIdleTimeout	Number	The number of minutes that the station can remain idle (not transmit payload traffic) before its session is terminated. This applies to stations that have authenticated to the network. Unless address space is at a premium, this can and should be set to a higher value than preAuthenticatedIdleTimeout. The default for this attribute is 30 minutes. This is an advanced option. An administrator should have to drill down for it in GUI applications. Validations: An integer between 0 and 999999.
preAuthenticatedIdleTimeout	Number	The number of minutes that the station can remain idle (not transmit payload traffic) before its session is terminated. Applies to stations in the unauthenticated state. Usually this should be set to a low value since many devices associate to whatever wireless networks they see, even though the owner is not planning to use the network and may not be aware that there even is a wireless network nearby. The default for this attribute is 5 minutes. This is an advanced option. An administrator should have to drill down for it in GUI applications. Validations: An integer between 5 and 999999.
privacyWpaPassPhrase	String	A string to contain the WPA-PSK passphrase.
redirectOrigDestOnSuccess	Boolean	Flag to specify to redirect Pronto CP users to their original destination upon successful login.
rejectOnRadiusTimeout	Boolean	A flag to reject MU if a RADIUS request times out.
rm11kBeaconReport	Boolean	Select to enable the beacon report.
rm11kQuietIe	Boolean	Select to enable Quiet IE.
rm11ksupport	Boolean	Select to enable 11rSupport.
roamingAssistPolicy	Boolean	A flag to enable client roaming assistance for legacy clients (not 802.11v complaint).

Table 23: Request Attributes (continued)

Attribute	Data Type	Description
serviceName	String	The unique service name defined by the user. Validations: A not null and non-empty string, between 1 to 64 characters. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
sessionTimeout	Number	The maximum number of minutes that a station is allowed to have a session on the network before it is logged out. This applies even when the user is active. Setting this to 0 allows the user to stay on the network indefinitely without reauthenticating. The default for this attribute is 0. This value is used as the default maximum session duration for each new session. The session duration timeout values sent from a RADIUS server overrides this value. Validations: An integer between 0 and 999999.
ssid	String	The SSID is not necessarily the same as the service name, but the service name is the default for the SSID. Validations: A not null and non-empty string, between 1 to 32 characters. Valid character set: Alphanumeric and special characters.
status	ServiceStatus	The status of the service (enabled, disabled, scheduled).
suppressSsid	Boolean	Include the SSID in the beacon frame or suppress it. Setting this attribute to true prevents the SSID from being advertised in the beacon. Setting it to false requires the SSID to be included in the beacon advertisements. (This should be considered an advanced option for an administrator.) Default: false
tag	String	An arbitrary identifier of SSID. Examples: guest or staff
uapsdEnabled	Boolean	Unscheduled Automatic Power Save Delivery (U-APSD) also known as WMM power save. Set to true to enable U-APSD and false to disable. (This is an advanced setting that most users will never need to change. It is configurable only because some client devices do not implement U-APSD correctly and run into trouble on networks using it.) Default: true (enabled)
unAuthenticatedUserDefaultRoleID	String	Default role for unauthenticated users.
vendorSpecificAttributes	Array of VsaTypes	In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Extreme Networks IdentifiFi Wireless authentication mechanism provides seven VSAs for RADIUS and other authentication mechanisms.

- 3 Assign the network to an existing site.

```
PUT http://ipAddress/management/v3/sites/siteID
```

Example: POST Request - Create a Network

```
{
```

```

"custId":"1-25R001C",
"id":"f0e17380-a870-11e7-8fd1-a34beb33e832",
"serviceName":"Service_1",
"status":"enabled","ssid":"Service_1",
"defaultTopology":"87b7f72c-8fcb-11e5-8994-feff819cdc9f",
"defaultCoS":"86500336-ed48-11e5-9ce9-5e5517507c66",
"flexibleClientAccess":false,
"privacy":null,
"privacyWpaPassPhrase":null,
"enabledSchedule":null,
"suppressSsid":false,
"mgmtFrameProtection":"enabled",
"enabled11kSupport":false,
"preAuthenticatedIdleTimeout":300,
"postAuthenticatedIdleTimeout":1800,
"sessionTimeout":0,
"uapsdEnabled":false,
"rmlkSupport":false,
"rmlkBeaconReport":false,
"rmlkQuietIe":false,
"admissionControlVideo":false,
"admissionControlVoice":false,
"admissionControlBestEffort":false,
"admissionControlBackgroundTraffic":false,
"airtimeFairness":false,
"mbaAuthorization":false,
"vendorSpecificAttributes":[],
"mbatimeoutRoleId":null,
"enableCaptivePortal":false,
"unAuthenticatedUserDefaultRoleId":"91f27cd0-8fcb-11e5-8994-feff819cdc9f",
"authenticatedUserDefaultRoleId":"91f27cd0-8fcb-11e5-8994-feff819cdc9f",
"features":["APP-CONTROL","CP-AT-AP","CP-AT-AP-PRONTO","IPV6","WIRED-PORTS"],
"captivePortalId":null,
  "rejectOnRadiusTimeout":true,
"policyOnRadiusTimeout":null,
"tag":null,"aaaPolicy":null,
"azaraCos":null,
"bridgingMode":"local",
"roamingAssistPolicy":false,
"clientToClientCommunication":false,
"openDNSDeviceId":null,
"clientLoadBalancing":false,
"classification":"wmm",
"captivePortalType":"CPTYPE_NONE",
"redirectOrigDestOnSuccess":true
}

```

Example: Response - Create a Network

```

{
"custId":"1-25R001C","id":"f0e17380-a870-11e7-8fd1-a34beb33e832",
"serviceName":"Service_1",
"status":"enabled","ssid":"Service_1",
"defaultTopology":"87b7f72c-8fcb-11e5-8994-feff819cdc9f",
"defaultCoS":"86500336-ed48-11e5-9ce9-5e5517507c66",
"flexibleClientAccess":false,
"privacy":null,
"privacyWpaPassPhrase":null,
"enabledSchedule":null,

```

```

"suppressSsid":false,
"mgmtFrameProtection":"enabled",
"enabled11kSupport":false,
"preAuthenticatedIdleTimeout":300,
"postAuthenticatedIdleTimeout":1800,
"sessionTimeout":0,
"uapsdEnabled":false,
"rm11kSupport":false,
"rm11kBeaconReport":false,
"rm11kQuietIe":false,
"admissionControlVideo":false,
"admissionControlVoice":false,
"admissionControlBestEffort":false,
"admissionControlBackgroundTraffic":false,
"airtimeFairness":false,
"mbaAuthorization":false,
"vendorSpecificAttributes":[],
"mbatimeoutRoleId":null,
"enableCaptivePortal":false,
"unAuthenticatedUserDefaultRoleID":"91f27cd0-8fcb-11e5-8994-feff819cdc9f",
"authenticatedUserDefaultRoleID":"91f27cd0-8fcb-11e5-8994-feff819cdc9f",
"features":["APP-CONTROL","CP-AT-AP","CP-AT-AP-PRONTO","IPV6","WIRED-PORTS"],
"captivePortalId":null,
"rejectOnRadiusTimeout":true,
"policyOnRadiusTimeout":null,
"tag":null,"aaaPolicy":null,
"azaraCos":null,
"bridgingMode":"local",
"roamingAssistPolicy":false,
"clientToClientCommunication":false,
"openDNSDeviceId":null,
"clientLoadBalancing":false,
"classification":"wmm",
"captivePortalType":"CPTYPE_NONE",
"redirectOrigDestOnSuccess":true
}

```

Example: PUT Request - Update a Site

```

{
  "custId":"1-25R001C",
  "id":"0c891450-a85b-11e7-8fd1-a34beb33e832",
  "siteName":"Default",
  "country":"UNITED_STATES",
  "timezone":"America/New_York",
  "scheduleUpgradeInfo":{
    "custId":null,
    "id":null,
    "preferredDayOfWeek":null,
    "preferredWeek":null,
    "preferredTime":{
      "custId":null,
      "id":null,
      "hour":0,
      "minute":0
    }
  },
  "siteManagerName":null,
  "siteManagerEmail":null,
  "contact":null,
  "smartRFPolicy":{
    "custId":null,

```

```

    "id":null,
    "txMinimumPower5":3,
    "txMaximumPower5":16,
    "txMinimumPower24":3,
    "txMaximumPower24":16,
    "acsChannelSelection5":"CHPLAN_ALLBYCOUNTRY",
    "acsChannelSelectionList5":
["157+1/40","100/40","140+1/40","132+1/40","140/40","108/40","36/40","165/40","100+1/40","
132/40","149+1/40","157/40","44/40","149/40","60+1/40","108+1/40","116+1/40","52/40","124/
40","124+1/40","44+1/40","52+1/40","36+1/40","116/40","60/40"],
    "acsChannelSelection24":"CHPLAN_AUTO",
    "acsChannelSelectionList24":["11","1","6"],
    "dot11nChannelWidth5":"Ch1Width_40MHz",
    "dot11nChannelWidth24":"Ch1Width_20MHz",
    "rfSensitivity":"medium",
    "ocsClientAware24":0,
    "ocsClientAware5":0,
    "ocsVoiceAware24":"dynamic",
    "ocsVoiceAware5":"dynamic",
    "interferenceRecovery":true,
    "coverageHoleRecovery":true,
    "neighborRecovery":true,
    "minInterferenceChannelSwitch5":20,
    "minInterferenceChannelSwitch24":20,
    "minSnrThreshold5":20,
    "minSnrThreshold24":20,
    "runOcsScanOncePerDay":false,
    "dcsNoiseInterferenceThreshold5":-80,
    "dcsChannelOccupanyThreshold5":100,
    "dcsUpdatePeriod5":5,
    "dcsNoiseInterferenceThreshold24":-80,
    "dcsChannelOccupanyThreshold24":100,
    "dcsUpdatePeriod24":5,"interferenceWaitTime24":10
  },
  "managementPolicy":{
    "custId":null,
    "id":null,
    "name":null,"adminPassword":null,
    "enableTraps":false,
    "snmpTrapReceivers":[],
    "snmpUSMs":[]
  },
  "deviceGroups":[{
    "custId":null,
    "id":"0c891450-a85b-11e7-8fd1-a34beb33e832",
    "groupName":null,
    "loadBalanceBandPreferenceEnabled":false,
    "roleIDs":["148c4042-efb0-11e5-9ce9-5e5517507c66","91f27cd0-8fcb-11e5-8994-
feff819cdc9f","0c1c48c0-a85b-11e7-8fd1-a34beb33e832","26820c30-a870-11e7-8fd1-
a34beb33e832"],
    "apSerialNumbers":["1549Y-1019600000"],
    "switchSerialNumbers":["1551N-40607"],
    "topologyIDs":["87b7f72c-8fcb-11e5-8994-feff819cdc9f"],
    "serviceIDs":[],
    "backboneTopologyIDs":[],
    "radioAssignment":[{
      "serviceId":"0c602f90-a85b-11e7-8fd1-a34beb33e832",
      "radioBand":"Band5"
    }, {
      "serviceId":"0c602f90-a85b-11e7-8fd1-a34beb33e832",
      "radioBand":"Band24"
    }, {
      "serviceId":"f0e17380-a870-11e7-8fd1-a34beb33e832",
      "radioBand":"Band5"
    }
  ]
}

```

```

    }, {
      "serviceId": "f0e17380-a870-11e7-8fd1-a34beb33e832",
      "radioBand": "Band24"
    } ],
    "wiredInterfaceAssignment": [],
    "enableDpi": true, "minimumBaseRate2_4": 6,
    "minimumBaseRate5": 6,
    "aggregateMpdu2_4": true,
    "aggregateMpdu5": true,
    "stbcEnabled2_4": false,
    "stbcEnabled5": false,
    "txbfEnabled2_4": "disabled",
    "txbfEnabled5": "muMimo",
    "dnsServers": ["0.0.0.0"]
  } ],
  "treeNode": {
    "custId": null,
    "id": null, "country": null,
    "region": null,
    "campus": null,
    "city": null,
    "mapCoordinates": null
  },
  "snmpConfig": {
    "custId": null,
    "id": null,
    "snmpVersion": "DISABLED",
    "v2Communities": {},
    "v3Users": [],
    "notifications": []
  },
  "syslogConfiguration": {
    "custId": null,
    "id": null,
    "enabled": false,
    "logging": "INFO",
    "syslogConfig": {"": 514},
    "logGuestTraffic": false
  },
  "siteType": "IDENTIFI",
  "features": ["APP-CONTROL", "CP-AT-AP", "CP-AT-AP-PRONTO", "IPV6", "WIRED-PORTS"], "floorIds":
[]
}

```

Example: Response - Update a Site

```

{
  "custId" : "1-25R001C",
  "id" : "0c891450-a85b-11e7-8fd1-a34beb33e832",
  "siteName" : "Default",
  "country" : "UNITED_STATES",
  "timezone" : "America/New_York",
  "scheduleUpgradeInfo" : {
    "custId" : null,
    "id" : null,
    "preferredDayOfWeek" : null,
    "preferredWeek" : null,
    "preferredTime" : {
      "custId" : null,
      "id" : null,
      "hour" : 0,
      "minute" : 0
    }
  }
}

```

```

},
"siteManagerName" : null,
"siteManagerEmail" : null,
"contact" : null,
"smartRFPolicy" : {
  "custId" : null,
  "id" : null,
  "txMinimumPower5" : 3,
  "txMaximumPower5" : 16,
  "txMinimumPower24" : 3,
  "txMaximumPower24" : 16,
  "acsChannelSelection5" : "CHPLAN_ALLBYCOUNTRY",
  "acsChannelSelectionList5" : [ "157+1/40", "100/40", "140+1/40", "132+1/40",
"140/40", "108/40", "36/40", "165/40", "100+1/40", "132/40", "149+1/40", "157/40",
"44/40", "149/40", "60+1/40", "108+1/40", "116+1/40", "52/40", "124/40", "124+1/40",
"44+1/40", "52+1/40", "36+1/40", "116/40", "60/40" ],
  "acsChannelSelection24" : "CHPLAN_AUTO",
  "acsChannelSelectionList24" : [ "11", "1", "6" ],
  "dot11nChannelWidth5" : "Ch1Width_40MHz",
  "dot11nChannelWidth24" : "Ch1Width_20MHz",
  "rfSensitivity" : "medium",
  "ocsClientAware24" : 0,
  "ocsClientAware5" : 0,
  "ocsVoiceAware24" : "dynamic",
  "ocsVoiceAware5" : "dynamic",
  "interferenceRecovery" : true,
  "coverageHoleRecovery" : true,
  "neighborRecovery" : true,
  "minInterferenceChannelSwitch5" : 20,
  "minInterferenceChannelSwitch24" : 20,
  "minSnrThreshold5" : 20,
  "minSnrThreshold24" : 20,
  "runOcsScanOncePerDay" : false,
  "dcsNoiseInterferenceThreshold5" : -80,
  "dcsChannelOccupancyThreshold5" : 100,
  "dcsUpdatePeriod5" : 5,
  "dcsNoiseInterferenceThreshold24" : -80,
  "dcsChannelOccupancyThreshold24" : 100,
  "dcsUpdatePeriod24" : 5,
  "interferenceWaitTime24" : 10
},
"managementPolicy" : {
  "custId" : null,
  "id" : null,
  "name" : null,
  "adminPassword" : null,
  "enableTraps" : false,
  "snmpTrapReceivers" : [ ],
  "snmpUSMs" : [ ]
},
"deviceGroups" : [ {
  "custId" : null,
  "id" : "0c891450-a85b-11e7-8fd1-a34beb33e832",
  "groupName" : null,
  "loadBalanceBandPreferenceEnabled" : false,
  "roleIDs" : [ "148c4042-efb0-11e5-9ce9-5e5517507c66", "91f27cd0-8fcb-11e5-8994-
feff819cdc9f", "0c1c48c0-a85b-11e7-8fd1-a34beb33e832", "26820c30-a870-11e7-8fd1-
a34beb33e832" ],
  "apSerialNumbers" : [ "1549Y-1019600000" ],
  "switchSerialNumbers" : [ "1551N-40607" ],
  "topologyIDs" : [ "87b7f72c-8fcb-11e5-8994-feff819cdc9f" ],
  "serviceIDs" : [ "0c602f90-a85b-11e7-8fd1-a34beb33e832", "f0e17380-a870-11e7-8fd1-
a34beb33e832" ],
  "backboneTopologyIDs" : [ ],

```



```

"radioAssignment" : [ {
  "custId" : null,
  "id" : null,
  "serviceId" : "0c602f90-a85b-11e7-8fd1-a34beb33e832",
  "radioBand" : "Band5"
}, {
  "custId" : null,
  "id" : null,
  "serviceId" : "0c602f90-a85b-11e7-8fd1-a34beb33e832",
  "radioBand" : "Band24"
}, {
  "custId" : null,
  "id" : null,
  "serviceId" : "f0e17380-a870-11e7-8fd1-a34beb33e832",
  "radioBand" : "Band5"
}, {
  "custId" : null,
  "id" : null,
  "serviceId" : "f0e17380-a870-11e7-8fd1-a34beb33e832",
  "radioBand" : "Band24"
} ],
"wiredInterfaceAssignment" : [ ],
"enableDpi" : true,
"minimumBaseRate2_4" : 6,
"minimumBaseRate5" : 6,
"aggregateMpdu2_4" : true,
"aggregateMpdu5" : true,
"stbcEnabled2_4" : false,
"stbcEnabled5" : false,
"txbfEnabled2_4" : "disabled",
"txbfEnabled5" : "muMimo",
"dnsServers" : [ "0.0.0.0" ]
} ],
"treeNode" : {
  "custId" : null,
  "id" : null,
  "country" : null,
  "region" : null,
  "campus" : null,
  "city" : null,
  "mapCoordinates" : null
},
"snmpConfig" : {
  "custId" : null,
  "id" : null,
  "snmpVersion" : "DISABLED",
  "v2Communities" : { },
  "v3Users" : [ ],
  "notifications" : [ ]
},
"syslogConfiguration" : {
  "custId" : null,
  "id" : null,
  "enabled" : false,
  "logging" : "INFO",
  "syslogConfig" : { },
  "logGuestTraffic" : false
},
"siteType" : "IDENTIFI",
"features" : [ "APP-CONTROL", "CP-AT-AP", "CP-AT-AP-PRONTO", "IPV6", "WIRED-PORTS" ],
"floorIds" : [ ]
}

```

Assign Port Functions

This procedure outlines how to assigning specific port functions to switch ports.

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To assign specific port functions:

- 1 Log in to the REST API server (api.ezcloudx.com) using administrator credentials. You must also forward the credentials with each API call. For an example of how to log in, see [Log in to the REST API Server](#) on page 234.
- 2 Use the GET method to specify a switch by serial number and view the list of ports for that switch:

```
GET http://{ipAddress}/v1/switches/{serialNumber}/ports
```

- 3 Update the switch ports by assigning functions to its ports:

```
PUT HTTP://{ipAddress}/v1/switches/{serialNumber}/ports/{portNumber}
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- content-type: application/json ;charset=UTF-8
- accept: application/json, text/plain, /*/*

Any of the following Accept headers are allowed with the Content-Type header request header:

- accept: application/json
- accept-encoding: gzip, deflate, br
- accept-language: en-US,en;q=0.8,und;q=0.6

Table 24: Request Attributes

Attribute	Data Type	Description
adminStatus	PortAdminStatus	Supports administratively enable and disabling a port. Validations: One of the values from the PortAdminStatus enum On/Off.
defaultPolicy	String	The default policy assigned to the port.
isDot1xEnabled	Boolean	A flag to indicate if Dot1x is enabled on the port. Valid values are true/false.
isLLDPEnabled	Boolean	A flag to indicate if LLDP is enabled on the port. Valid values are true/false.
isMacAuthEnabled	Boolean	A flag to indicate if MAC based authentication is enabled on the port. Valid values are true/false.
isSTPEnabled	Boolean	A flag to indicate if STP is enabled on the port. Valid values true/false.

Table 24: Request Attributes (continued)

Attribute	Data Type	Description
lagType	LagPortType	A flag to identify if a port is LAG master or member port.
lagmembers	Array of strings	A list of lag member ports.
poePortConfig	PoEPortElement	The POE configuration on the port.
portAlias	String	The user assigned name for the port. ExtremeCloud will auto generate "portAliases" to be the serial number of the device + port ID, and will not allow the user to set the port (this is to match ZTP+ implementation). Validations: Not required, as it is a read only attribute.
portCapability	SwitchPortCapabilityElement	Returns the capability, software/hardware of a switch port.
portName	String	The name of the port. Default Name: portNumber.
portNumber	String	The name of the port, for XOS is the numeric value matching port ID (on the CLI). Validations: Not required, as it is a read only attribute.
portSpeed	PortSpeedEnum	The actual port speed. Validations: A valid type of PortSpeedEnum.
portType	PortType	The type of the port. Supported values are Access/Uplink/Others. Validations: Not required, as it is a read only attribute.
pvid	String	The port VLAN ID.
taggedTopologies	Array of string	A list of tagged topologies configured in a site.
untaggedTopology	String	The untagged topologies configured in a site.
features	Array of strings	A list of supported features.
flexibleClientAccess	Boolean	Enabling this feature causes an access point (AP) to take steps to ensure that fast clients with content to send will get as much airtime as slow clients. When this is feature is turned off, the AP treats all clients equally and processes packet forwarding requests on a First-Come-First-Serve basis. Default: disable
mbaAuthorization	Boolean	Select to enable MBA authorization.
mbatimeoutRoleId	String	The MAC-based authentication timeout role ID. Validations: A valid UUID of a role.
mgmtFrameProtection	MgmtFrameProtection	The management frame protection to use (disabled/enabled/required).
openDNSDeviceId	String	Content filtering using open DNS.
policyOnRadiusTimeout	String	A role to apply if the rejectonradiustimeout = false and the RADIUS request times out.

Table 24: Request Attributes (continued)

Attribute	Data Type	Description
postAuthenticatedIdleTimeout	Number	The number of minutes that the station can remain idle (not transmit payload traffic) before its session is terminated. This applies to stations that have authenticated to the network. Unless address space is at a premium, this can and should be set to a higher value than preAuthenticatedIdleTimeout. The default for this attribute is 30 minutes. This is an advanced option. An administrator should have to drill down for it in GUI applications. Validations: An integer between 0 and 999999.
preAuthenticatedIdleTimeout	Number	The number of minutes that the station can remain idle (not transmit payload traffic) before its session is terminated. Applies to stations in the unauthenticated state. Usually this should be set to a low value since many devices associate to whatever wireless networks they see, even though the owner is not planning to use the network and may not be aware that there even is a wireless network nearby. The default for this attribute is 5 minutes. This is an advanced option. An administrator should have to drill down for it in GUI applications. Validations: An integer between 5 and 999999.
privacyWpaPassPhrase	String	A string to contain the WPA-PSK passphrase.
redirectOrigDestOnSuccess	Boolean	Flag to specify to redirect Pronto CP users to their original destination upon successful login.
rejectOnRadiusTimeout	Boolean	A flag to reject MU if a RADIUS request times out.
rm11kBeaconReport	Boolean	Select to enable the beacon report.
rm11kQuietIE	Boolean	Select to enable Quiet IE.
rm11ksupport	Boolean	Select to enable 11r support.
roamingAssistPolicy	Boolean	A flag to enable client roaming assistance for legacy clients (not 802.11v compliant).
serviceName	String	The unique service name defined by the user. Validations: A not null and non-empty string, between 1 to 64 characters. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
sessionTimeout	Number	The maximum number of minutes that a station is allowed to have a session on the network before it is logged out. This applies even when the user is active. Setting this to 0 allows the user to stay on the network indefinitely without reauthenticating. The default for this attribute is 0. This value is used as the default maximum session duration for each new session. The session duration timeout values sent from a RADIUS server overrides this value. Validations: An integer between 0 and 999999.

Table 24: Request Attributes (continued)

Attribute	Data Type	Description
ssid	String	The SSID is not necessarily the same as the service name, but the service name is the default for the SSID. Validations: A not null and non-empty string, between 1 to 32 characters. Valid character set: Alphanumeric and special characters.
status	ServiceStatus	The status of the service (enabled, disabled, scheduled).
suppressSsid	Boolean	Include the SSID in the beacon frame or suppress it. Setting this attribute to true prevents the SSID from being advertised in the beacon. Setting it to false requires the SSID to be included in the beacon advertisements. (This should be considered an advanced option for an administrator.) Default: false
tag	String	An arbitrary identifier of SSID. Examples: guest or staff
uapsdEnabled	Boolean	Unscheduled Automatic Power Save Delivery (U-APSD) also known as WMM power save. Set to true to enable U-APSD and false to disable. (This is an advanced setting that most users will never need to change. It is configurable only because some client devices do not implement U-APSD correctly and run into trouble on networks using it.) Default: true (enabled)
unAuthenticatedUserDefaultRoleID	String	Default role for unauthenticated users.
vendorSpecificAttributes	Array of VsaTypes	In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Extreme Networks IdentifiFi Wireless authentication mechanism provides seven VSAs for RADIUS and other authentication mechanisms.

Example: PUT Request - Update Port Functions on a Switch

```
{
  "custId":null,
  "id":null,
  "portNumber":"7",
  "portName":"7",
  "portType":"ACCESS",
  "portAlias":"7",
  "portSpeed":"AUTO",
  "typeOfService":0,
  "adminStatus":"On",
  "defaultPolicy":null,
  "poePortConfig":{
    "custId":null,
    "id":null,
    "portName":"7",
    "enabled":false,
    "poePortAlias":"7",
    "detection":"poe_802_3af_only",
    "operatorLimit":null,"priority":null
  },
}
```

```

"lagmembers": [],
"lagType": "None",
"taggedTopologies": [],
"untaggedTopology": "87b7f72c-8fcb-11e5-8994-feff819cdc9f",
"portCapability": {
  "custId": null,
  "id": null,
  "speedsSupported": ["AUTO", "SPEED_1GIG", "SPEED_TEN100", "TEN"],
  "poeSupported": false, "mediaType": "Copper_1G"
},
"pvid": "87b7f72c-8fcb-11e5-8994-feff819cdc9f",
"stpenabled": true,
"lldpenabled": true,
"dot1xEnabled": true,
"macAuthEnabled": false
}

```

Example: Response - Update Port Functions on a Switch

```

{
  "custId" : null,
  "id" : null,
  "portNumber" : "7",
  "portName" : "7",
  "portType" : "ACCESS",
  "portAlias" : "7",
  "portSpeed" : "AUTO",
  "typeOfService" : 0,
  "adminStatus" : "On",
  "defaultPolicy" : null,
  "poePortConfig" : {
    "custId" : null,
    "id" : null,
    "portName" : "7",
    "enabled" : false,
    "poePortAlias" : "7",
    "detection" : "poe_802_3af_only",
    "operatorLimit" : null,
    "priority" : null
  },
  "lagmembers" : [ ],
  "lagType" : "None",
  "taggedTopologies" : [ ],
  "untaggedTopology" : "87b7f72c-8fcb-11e5-8994-feff819cdc9f",
  "portCapability" : {
    "custId" : null,
    "id" : null,
    "speedsSupported" : [ "AUTO", "SPEED_1GIG", "SPEED_TEN100", "TEN" ],
    "poeSupported" : false,
    "mediaType" : "Copper_1G"
  },
  "pvid" : "87b7f72c-8fcb-11e5-8994-feff819cdc9f",
  "stpenabled" : true,
  "lldpenabled" : true,
  "dot1xEnabled" : true,
  "macAuthEnabled" : false
}

```

Update an Access Point's Configuration

This procedure outlines how to update the attributes of an access point (AP), such as the site assignment.

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To update an access point's configuration:

- 1 Log in to the REST API server (api.ezcloudx.com) using administrator credentials. You must also forward the credentials with each API call. For an example of how to log in, see [Log in to the REST API Server](#) on page 234.
- 2 Get the list of APs to find the serial number of the AP you want to configure:

```
GET HTTP://ipAddress/v1/aps/
```

- 3 Change the configuration using the PUT method:

```
PUT HTTP://ipAddress/v1/aps/serialNumber
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- content-type: application/json ;charset=UTF-8
- accept: application/json, text/plain, */*

Any of the following Accept headers are allowed with the Content-Type header request header:

- accept: application/json
- accept-encoding: gzip, deflate, br
- accept-language: en-US,en;q=0.8,und;q=0.6

Table 25: Request Attributes: AccessPointElement

Attribute	Data Type	Description
apName	String	A user friendly name for the access point. (It defaults to the serial number and does not have to be unique.) Validations: The access point name must be between 0 and 64 characters long. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
baseService	License Mode	The base service associated with the AP.

Table 25: Request Attributes: AccessPointElement (continued)

Attribute	Data Type	Description
description	String	A user-entered string describing this access point (AP). Its contents can be completely arbitrary. It can be null or empty. Validations: The description must be between 0 and 255 characters long. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
deviceGroupld	String	The site associated with the AP.
dnsServers	Array of InetAddress	A list containing the list of DNS servers.
features	Array of strings	A list of supported features on the AP. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
floorld	String	The floor configured for the AP.
hardwareType	String	The model number of the device. The model number is a human readable string and is likely how the device is referred to in the customer documentation and data sheets. In the case of access points (APs), the model number provides critical information regarding the regulatory domain that the AP is to operate in, and provides a way to infer the number of radios in the AP and their capabilities. Validations: The hardware type value must be between 0 and 32 characters long. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
hostSite	String	The site to which the access point is associated. Validations: The software version must be between 0 and 64 characters long. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.

Table 25: Request Attributes: AccessPointElement (continued)

Attribute	Data Type	Description
ipAddress	InetAddress	The IP address of one of the access point's wired interfaces. This is the address of the AP on the customer's network. It is not the address that the cloud data center sees as the source when the AP sends a message to it. That address is likely to belong to a firewall/NAT. Validations: This value must be a valid IpAddress.
ipRoutes	Array of IpRouteElement	A list containing the IP routes.
lag	Status	The state the LAG should be in.
ledStatus	LedStatus	The state that the access point's LEDs should be in. It can be read or written. The default is "normal". Validations: A not null value.
logEnabled	Boolean	
radios	Array of RadioElement	A list of radios in the access point. Validations: A not null and non-empty list of RadioElements.
serialNumber	String	The globally unique serial number of the device being registered. The serial number is represented as a string. The actual length and format of the string depends on the type of device being registered. This is the only attribute of the device that must not be null. Validations: A not null and non-empty string having exactly 16 characters. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
services	Array of string	A list of the names of the services that this AP is providing. They could be obtained by looking up its site and getting them from there but it is likely that it will be more efficient to include references to the services directly. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
siteId	String	Site associated with the AP.

Table 25: Request Attributes: AccessPointElement (continued)

Attribute	Data Type	Description
softwareVersion	String	The software version number that is installed on the access point. Validations: There is no need for a user to enter this, so there is no need to validate it. Valid character set: Alphanumeric and special characters, except semi-colon, colon, and ampersand.
supportedCountries	Array of countries	A list of supported countries for the AP. Validations: None.
telnetEnabled	Boolean	A flag to enable and disable SSH.
vlanInterfaces	Array of VlanInterfaceElement	A list of VLAN interfaces configured on the access point.
wiredInterfaces	Array of WiredInterfaceElement	A list of wired interfaces configured on the access point.

Example: PUT Request

```
{ "custId": "MspEndCustomer-tenantid-zFj0XX0xXXxxX0xx",
  "id": null,
  "serialNumber": "0000Y-0000000000",
  "hardwareType": "AP3935i-FCC",
  "apName": "0000Y-0000000000",
  "softwareVersion": null,
  "currentAssets": [],
  "desiredAssets": [],
  "hostSite": "Default",
  "description": "update description",
  "services": ["Staff"],
  "ipAddress": null,
  "radios": [{"custId": null,
    "id": null,
    "radioIndex": 0,
    "mode": "anc",
    "channelwidth": "Ch1Width_40MHz",
    "adminState": true,
    "useSmartRf": true,
    "txMaxPower": 16,
    "txMinPower": 0,
    "antennaGain": 0,
    "environment": "INDOOR",
    "channel": "Auto",
    "requestedChannel": null,
    "acsChannelPlan": "ChannelPlanAllNonDFS",
    "automaticTransmitPowerControl": "disabled",
    "aggregateMpdu": null,
    "txBf": null,
    "stbc": null,
    "customAcsList": [],
    "dot11nChannelBonding": 0,
    "name": "1", "attenuation": 0},
  {"custId": null,
    "id": null,
    "radioIndex": 0,
    "mode": "gn",
```

```

    "channelwidth":"Ch1Width_20MHz",
    "adminState":true,
    "useSmartRf":true,
    "txMaxPower":16,
    "txMinPower":0,
    "antennaGain":0,
    "environment":"INDOOR",
    "channel":"Auto",
    "requestedChannel":null,
    "acsChannelPlan":"ChannelPlanAuto",
    "automaticTransmitPowerControl":"disabled",
    "aggregateMpdu":null,
    "txBf":null,
    "stbc":null,
    "customAcsList":[],
    "dot11nChannelBonding":0,
    "name":"2",
    "attenuation":0}},
"wiredInterfaces":[{"custId":null,
  "id":null,
  "name":"Uplink",
  "nativeVlan":1}],
"vlanInterfaces":[{"custId":null,
  "id":null,
  "vlanId":1,
"vlanIPAddresses":[{"ipAddress":"dhcp",
  "isSecondaryIPAddress":false}]}],
"logEnabled":false,
"ipRoutes":[],
"ledStatus":"NORMAL",
"sshAccessEnable":false,
"rootPassword":null,
"telnetEnabled":false,
"lag":"disabled",
"supportedCountries":["UNITED_STATES","COLOMBIA","PUERTO_RICO"],
"features":[],
"floorId":null,
"siteId":"8675309-00xx-00xx-00xx-8675309",
"deviceGroupId":null,
"baseService":"LICENSED",
"dnsServers":[],
"apAntennaModels":[]

```

Example: Response

```

{"custId":"MspEndCustomer-tenantid-zFj0XX0xXXxxX0xx",
  "id":null,
  "serialNumber":"0000Y-0000000000",
  "hardwareType":"AP3935i-FCC",
  "apName":"0000Y-0000000000",
  "softwareVersion":null,
  "currentAssets":[],
  "desiredAssets":[],
  "hostSite":"Default",
  "description":"update description",
  "services":["Staff"],
  "ipAddress":null,
  "radios":[{"custId":null,
    "id":null,
    "radioIndex":0,
    "mode":"anc",
    "channelwidth":"Ch1Width_40MHz",
    "adminState":true,
    "useSmartRf":true,

```

```

    "txMaxPower":16,
    "txMinPower":0,
    "antennaGain":0,
    "environment":"INDOOR",
    "channel":"Auto",
    "requestedChannel":null,
    "acsChannelPlan":"ChannelPlanAllNonDFS",
    "automaticTransmitPowerControl":"disabled",
    "aggregateMpdu":null,
    "txBf":null,
    "stbc":null,
    "customAcсList":[],
    "dot11nChannelBonding":0,
    "name":"1","attenuation":0},
{"custId":null,
  "id":null,
  "radioIndex":0,
  "mode":"gn",
  "channelwidth":"Ch1Width_20MHz",
  "adminState":true,
  "useSmartRf":true,
  "txMaxPower":16,
  "txMinPower":0,
  "antennaGain":0,
  "environment":"INDOOR",
  "channel":"Auto",
  "requestedChannel":null,
  "acsChannelPlan":"ChannelPlanAuto",
  "automaticTransmitPowerControl":"disabled",
  "aggregateMpdu":null,
  "txBf":null,
  "stbc":null,
  "customAcсList":[],
  "dot11nChannelBonding":0,
  "name":"2",
  "attenuation":0}},
"wiredInterfaces":[{"custId":null,
  "id":null,
  "name":"Uplink",
  "nativeVlan":1}],
"vlanInterfaces":[{"custId":null,
  "id":null,
  "vlanId":1,
"vlanIPAddresses":[{"ipAddress":"dhcp",
  "isSecondaryIPAddress":false}}]},
"logEnabled":false,
"ipRoutes":[],
"ledStatus":"NORMAL",
"sshAccessEnable":false,
"rootPassword":null,
"telnetEnabled":false,
"lag":"disabled",
"supportedCountries":["UNITED_STATES","COLOMBIA","PUERTO_RICO"],
"features":[],
"floorId":null,
"siteId":"8675309-00xx-00xx-00xx-8675309",
"deviceGroupId":null,
"baseService":"LICENSED",
"dnsServers":[],
"apAntennaModels":[] }

```

Change a Preshared Key

This procedure outlines how to update the WPA preshared key privacy for a networks service.

Note



The attributes in this topic are a representative sample of what is available. For a complete list of attributes, elements, and resources, see the main documentation of the REST API. The documentation resides in a user interface that is accessed using this URL: http://api.extremenetworks.com/extremecloud/rest_api/index.html

To change a preshared key:

- 1 Log in to the REST API server (api.ezcloudx.com) using administrator credentials. You must also forward the credentials with each API call. For an example of how to log in, see [Log in to the REST API Server](#) on page 234.
- 2 Get the list of services to get the service ID you want to change:

```
GET HTTP://ipAddressmanagement/v1/services
```

- 3 Change the configuration using the PUT method:

```
PUT HTTP://ipAddress/management/v1/services/serviceId
```

When you POST or PUT data to the REST API, at minimum set the Content-Type header to application/json. However, you should generally specify two headers when you post the log in request.

Example:

- `content-type: application/json ;charset=UTF-8`
- `accept: application/json, text/plain, */*`

Any of the following Accept headers are allowed with the Content-Type header request header:

- `accept: application/json`
- `accept-encoding: gzip, deflate, br`
- `accept-language: en-US,en;q=0.8,und;q=0.6`

Table 26: Request Attributes: WpaPskElement

Attribute	Data Type	Description
isKeyHexEncoded	boolean	Indicates whether the shared key is a plain text string or an ASCII-encoded hex string which could include hex representations of binary data.
mode	WpaV2Mode	Whether to support legacy clients that only can use TKIP. Auto - means use AES when possible but use TKIP for clients that only speak TKIP. AES means only use AES encryption, even if it means that a TKIP only client cannot access the network. Default is "auto" but "aes" is more secure.

Table 26: Request Attributes: WpaPskElement (continued)

Attribute	Data Type	Description
pmfMode	PmfMode	Whether to encrypt a subset of management frame traffic as specified by 802.11w. Default: enable
presharedKey	string	The shared key used by all APs and all clients accessing a service that is protected with the settings of this WpaPsk object. The length must be between 8 and 64 characters inclusive. Valid character set: Alphanumeric and special characters.

Example: PUT Request

```
{
  "custId": "MspEndCustomer-tenantid-zFj0XX0xXXxxX0xx",
  "id": "0xx00000-00xx-00x0-xx00xx25-x00xxx00xxxx",
  "serviceName": "Staff",
  "status": "enabled",
  "ssid": "Staff",
  "defaultTopology": "00x0x00x-0xxx-00x0-0000-xxxx000xxx0x",
  "defaultCoS": null,
  "flexibleClientAccess": false,
  "privacy": {
    "WpaPskElement": {
      "custId": null,
      "id": null,
      "mode": "auto",
      "pmfMode": "enabled",
      "inputType": "ASCII",
      "presharedKey": "abcd1234",
      "enableTkip": false,
      "keyHexEncoded": false
    }
  },
  "privacyWpaPassPhrase": null,
  "enabledSchedule": null,
  "suppressSsid": false,
  "mgmtFrameProtection": "enabled",
  "enabled11kSupport": false,
  "preAuthenticatedIdleTimeout": 300,
  "postAuthenticatedIdleTimeout": 1800,
  "sessionTimeout": 0,
  "uapsdEnabled": false,
  "rm11ksupport": false,
  "rm11kBeaconReport": false,
  "rm11kQuietIe": false,
  "admissionControlVideo": false,
  "admissionControlVoice": false,
  "admissionControlBestEffort": false,
  "admissionControlBackgroundTraffic": false,
  "airtimeFairness": false,
  "mbaAuthorization": false,
  "vendorSpecificAttributes": [],
  "mbatimeoutRoleId": null,
  "enableCaptivePortal": false,
  "unAuthenticatedUserDefaultRoleId": "00x00xx0-0xxx-00x0-0000-xxxx000xxx0x",
  "authenticatedUserDefaultRoleId": "00x00xx0-0xxx-00x0-0000-xxxx000xxx0x",
  "features": ["APP-CONTROL", "CP-AT-AP", "CP-AT-AP-PRONTO", "IPV6", "WIRED-PORTS"],
  "captivePortalId": null,
  "rejectOnRadiusTimeout": true,
  "policyOnRadiusTimeout": null,
}
```

```

"tag":null,"aaaPolicy":null,
"azaraCos":null,
"bridgingMode":"local",
"roamingAssistPolicy":false,
"clientToClientCommunication":false,
"openDNSDeviceId":null,
"clientLoadBalancing":false,
"classification":"wmm",
"captivPortalType":"CPTYPE_NONE",
"redirectOrigDestOnSuccess":true,
"redirectHTTPS":false}

```

Example: Response

```

{"custId":"MspEndCustomer-tenantid-zFj0XX0xXXxxX0xx",
"id":"0xx00000-00xx-00x0-xx00xx25-x00xxx00xxxx",
"serviceName":"Staff",
"status":"enabled",
"ssid":"Staff",
"defaultTopology":"00x0x00x-0xxx-00x0-0000-xxxx000xxx0x",
"defaultCoS":null,
"flexibleClientAccess":false,
"privacy":{"WpaPskElement":{"custId":null,
"id":null,
"mode":"auto",
"pmfMode":"enabled",
"inputType":"ASCII",
"presharedKey":"abcd1234",
"enableTkip":false,"keyHexEncoded":false}},
"privacyWpaPassPhrase":null,
"enabledSchedule":null,
"suppressSsid":false,
"mgmtFrameProtection":"enabled",
"enabled11kSupport":false,
"preAuthenticatedIdleTimeout":300,
"postAuthenticatedIdleTimeout":1800,
"sessionTimeout":0,
"uapsdEnabled":false,
"rm11kSupport":false,
"rm11kBeaconReport":false,
"rm11kQuietIe":false,
"admissionControlVideo":false,
"admissionControlVoice":false,
"admissionControlBestEffort":false,
"admissionControlBackgroundTraffic":false,
"airtimeFairness":false,
"mbaAuthorization":false,
"vendorSpecificAttributes":[],
"mbatimeoutRoleId":null,
"enableCaptivePortal":false,
"unAuthenticatedUserDefaultRoleId":"00x00xx0-0xxx-00x0-0000-xxxx000xxx0x",
"authenticatedUserDefaultRoleId":"00x00xx0-0xxx-00x0-0000-xxxx000xxx0x",
"features":["APP-CONTROL","CP-AT-AP","CP-AT-AP-PRONTO","IPV6","WIRED-PORTS"],
"captivPortalId":null,
"rejectOnRadiusTimeout":true,
"policyOnRadiusTimeout":null,
"tag":null,"aaaPolicy":null,
"azaraCos":null,
"bridgingMode":"local",
"roamingAssistPolicy":false,
"clientToClientCommunication":false,
"openDNSDeviceId":null,
"clientLoadBalancing":false,
"classification":"wmm",

```

```
"captivePortalType":"CPTYPE_NONE",  
"redirectOrigDestOnSuccess":true,  
"redirectHTTPS":false}
```


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 Application Analytics

EAA, 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. EAA 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 EAA at <http://www.extremenetworks.com/product/extremeanalytics/>.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at <http://www.extremenetworks.com/product/management-center/>.

ExtremeCloud Appliance

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

The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge. Learn more about ExtremeCloud Appliance at <https://www.extremenetworks.com/product/extremecloud-appliance/>.

ExtremeCloud

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

ExtremeControl

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at <https://www.extremenetworks.com/product/extremecontrol/>.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800, and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at <http://www.extremenetworks.com/products/switching-routing/>.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at <http://www.extremenetworks.com/products/wireless/>.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, 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/>.