



ExtremeWireless™

ExtremeWireless™ V10.41.06 User Guide



Copyright © 2018 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

Software Licensing

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

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>

Table of Contents

Preface	7
Text Conventions.....	7
Safety Information.....	7
Sicherheitshinweise.....	8
Consignes De Sécurité.....	9
Providing Feedback to Us.....	10
Getting Help.....	11
Extreme Networks Documentation.....	11
Chapter 1: About This Guide	12
Who Should Use This Guide.....	12
How to Use This Guide.....	12
Chapter 2: Overview of the ExtremeWireless Solution	14
Introduction.....	14
Conventional Wireless LANs.....	15
Elements of the ExtremeWireless Solution.....	15
ExtremeWireless and Your Network.....	19
ExtremeWireless Appliance Product Family.....	29
Chapter 3: Configuring the ExtremeWireless Appliance	31
System Configuration Overview.....	31
Logging on to the ExtremeWireless Appliance.....	33
Wireless Assistant Home Screen.....	34
Working with the Basic Installation Wizard.....	39
Configuring the ExtremeWireless Appliance for the First Time.....	45
Using a Third-party Location-based Solution.....	95
Additional Ongoing Operations of the System.....	99
Chapter 4: Configuring the ExtremeWireless APs	101
Wireless AP Overview.....	101
Discovery and Registration.....	120
Viewing a List of All APs.....	125
Wireless AP Default Configuration.....	134
Configuring Wireless AP Properties.....	156
Outdoor Access Point Installation.....	167
Assigning Wireless AP Radios to a VNS.....	168
Configuring Wireless AP Radio Properties.....	174
Configuring IoT Applications.....	189
Setting Up the Wireless AP Using Static Configuration.....	199
Setting Up 802.1x Authentication for a Wireless AP.....	203
Configuring Co-Located APs in Load Balance Groups.....	213
Configuring an AP Cluster.....	220
Configuring an AP as a Guardian.....	221
Configuring a Captive Portal on an AP.....	222
AP3916ic Integrated Camera Deployment.....	226
Performing AP Software Maintenance.....	235
Understanding the ExtremeWireless LED Status.....	242

Chapter 5: Configuring Topologies.....	262
Topology Overview.....	262
Configuring the Admin Port.....	263
Configuring a Basic Data Port Topology.....	266
Creating a Topology Group.....	270
Edit or Delete a Topology Group.....	271
Enabling Management Traffic.....	272
Layer 3 Configuration.....	272
Exception Filtering.....	278
Multicast Filtering.....	281
Chapter 6: Configuring Roles.....	284
Roles Overview.....	284
Configuring Default VLAN and Class of Service for a Role.....	284
Policy Rules.....	288
Chapter 7: Configuring WLAN Services.....	318
WLAN Services Overview.....	318
Third-party AP WLAN Service Type.....	319
Configuring a Basic WLAN Service.....	319
Configuring Privacy.....	327
Configuring Accounting and Authentication.....	334
Configuring QoS Modes.....	370
Configuring Hotspots.....	376
Chapter 8: Configuring a VNS.....	390
Configuring a VNS.....	390
VNS Global Settings.....	392
Methods for Configuring a VNS.....	423
Manually Creating a VNS.....	423
Creating a VNS Using the Wizard.....	426
Enabling and Disabling a VNS.....	485
Renaming a VNS.....	486
Deleting a VNS.....	486
Chapter 9: Configuring Classes of Service.....	487
Classes of Service Overview.....	487
Configuring Classes of Service.....	487
CoS Rule Classification.....	490
Priority and ToS/DSCP Marking.....	491
Rate Limiting.....	492
Chapter 10: Configuring Sites.....	494
VNS Sites Overview.....	494
Configuring Sites.....	494
Recommended Deployment Guidelines.....	495
Radius Configuration.....	499
Selecting AP Assignments.....	500
Selecting WLAN Assignments.....	501
Chapter 11: Working with a Mesh Network.....	502
About Mesh.....	502

Simple Mesh Configuration.....	502
Wireless Repeater Configuration.....	503
Wireless Bridge Configuration.....	504
Examples of Deployment.....	505
Mesh WLAN Services.....	505
Key Features of Mesh.....	509
Deploying the Mesh System.....	511
Changing the Pre-shared Key in a Mesh WLAN Service.....	517
Chapter 12: Working with a Wireless Distribution System.....	518
About WDS.....	518
Simple WDS Configuration.....	518
Wireless Repeater Configuration.....	519
Wireless Bridge Configuration.....	520
Examples of Deployment.....	521
WDS WLAN Services.....	521
Key Features of WDS.....	525
Deploying the WDS System.....	528
Changing the Pre-shared Key in a WDS WLAN Service.....	536
Chapter 13: Availability and Session Availability.....	537
Availability.....	537
Session Availability.....	545
Viewing SLP Activity.....	553
Chapter 14: Configuring Mobility.....	555
Mobility Overview.....	555
Mobility Domain Topologies.....	556
Configuring a Mobility Domain.....	558
Chapter 15: Working with Third-party APs.....	561
Defining Authentication by Captive Portal for the Third-party AP WLAN Service.....	561
Defining the Third-party APs List.....	561
Defining Policy Rules for the Third-party APs.....	561
Chapter 16: Working with ExtremeWireless Radar.....	563
Radar Overview.....	563
Radar Components.....	564
Radar License Requirements.....	565
Enabling the Analysis Engine.....	565
Radar Scan Profiles.....	566
AirDefense Profile.....	567
Viewing Existing Radar Profiles.....	571
Adding a New Radar Profile.....	573
Configuring an In-Service Scan Profile.....	574
Configuring a Guardian Scan Profile.....	577
Assigning an AP to a Profile.....	581
Viewing the List of Assigned APs.....	581
Maintaining the Radar List of APs.....	582
Working with Radar Reports.....	593
Chapter 17: Working with Location Engine.....	605
Location Engine Overview.....	605

Location Engine on the Controller.....	607
Deploying APs for Location Aware Services.....	608
Configuring the Location Engine.....	609
ExtremeLocation Support.....	619
Chapter 18: Working with Reports and Statistics.....	621
Application Visibility and Device ID.....	621
Viewing AP Reports and Statistics.....	627
Available Client Reports.....	642
Viewing Role Filter Statistics.....	646
Viewing Topology Reports.....	648
Viewing Mobility Reports.....	650
Viewing Controller Status Information.....	654
Viewing Routing Protocol Reports.....	657
Viewing RADIUS Reports.....	660
Call Detail Records (CDRs).....	663
Chapter 19: Performing System Administration.....	669
Performing Wireless AP Client Management.....	669
Defining Wireless Assistant Administrators and Login Groups.....	673
Chapter 20: Logs, Traces, Audits and DHCP Messages.....	676
ExtremeWireless Appliance Messages.....	676
Working with Logs.....	676
Viewing Wireless AP Traces.....	684
Viewing Audit Messages.....	684
Viewing the DHCP Messages.....	685
Viewing the NTP Messages.....	686
Viewing Software Upgrade Messages.....	687
Viewing Configuration Restore/Import Messages.....	689
Chapter 21: Working with GuestPortal Administration.....	690
About GuestPortals.....	690
Adding New Guest Accounts.....	690
Enabling or Disabling Guest Accounts.....	693
Editing Guest Accounts.....	693
Removing Guest Accounts.....	694
Importing and Exporting a Guest File.....	695
Viewing and Printing a GuestPortal Account Ticket.....	698
Working with the Guest Portal Ticket Page.....	700
Configuring Guest Password Patterns.....	701
Configuring Web Session Timeouts.....	704
Appendix A: Regulatory Information.....	705
ExtremeWireless APs 37XX , 38XX, and 39XX.....	705
Appendix B: Default GuestPortal Ticket Page.....	706
Example Ticket Page.....	706
Glossary.....	709

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
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written 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.

Safety Information

Dangers

- Replace the power cable immediately if it shows any sign of damage.
- Replace any damaged safety equipment (covers, labels and protective cables) immediately.

- Use only original accessories or components approved for the system. Failure to observe these instructions may damage the equipment or even violate safety and EMC regulations.
- Only authorized Extreme Networks service personnel are permitted to service the system.

Warnings

- This device must not be connected to a LAN segment with outdoor wiring.
- Ensure that all cables are run correctly to avoid strain.
- Replace the power supply adapter immediately if it shows any sign of damage.
- Disconnect all power before working near power supplies unless otherwise instructed by a maintenance procedure.
- Exercise caution when servicing hot swappable components: power supplies or fans. Rotating fans can cause serious personal injury.
- This unit may have more than one power supply cord. To avoid electrical shock, disconnect all power supply cords before servicing. In the case of unit failure of one of the power supply modules, the module can be replaced without interruption of power to the ExtremeWireless Appliance. However, this procedure must be carried out with caution. Wear gloves to avoid contact with the module, which will be extremely hot.
- There is a risk of explosion if a lithium battery is not correctly replaced. The lithium battery must be replaced only by an identical battery or one recommended by the manufacturer.
- Always dispose of lithium batteries properly.
- Do not attempt to lift objects that you think are too heavy for you.

Cautions

- Check the nominal voltage set for the equipment (operating instructions and type plate). High voltages capable of causing shock are used in this equipment. Exercise caution when measuring high voltages and when servicing cards, panels, and boards while the system is powered on.
- Only use tools and equipment that are in perfect condition. Do not use equipment with visible damage.
- To protect electrostatic sensitive devices (ESD), wear a wristband before carrying out any work on hardware.
- Lay cables so as to prevent any risk of them being damaged or causing accidents, such as tripping.

Sicherheitshinweise

Gefahrenhinweise

- Sollte das Netzkabel Anzeichen von Beschädigungen aufweisen, tauschen Sie es sofort aus.
- Tauschen Sie beschädigte Sicherheitsausrüstungen (Abdeckungen, Typenschilder und Schutzkabel) sofort aus.
- Verwenden Sie ausschließlich Originalzubehör oder systemspezifisch zugelassene Komponenten. Die Nichtbeachtung dieser Hinweise kann zur Beschädigung der Ausrüstung oder zur Verletzung von Sicherheits- und EMV-Vorschriften führen.
- Das System darf nur von autorisiertem Extreme Networks-Servicepersonal gewartet werden.

Warnhinweise

- Dieses Gerät darf nicht über Außenverdrahtung an ein LAN-Segment angeschlossen werden.
- Stellen Sie sicher, dass alle Kabel korrekt geführt werden, um Zugbelastung zu vermeiden.
- Sollte das Netzteil Anzeichen von Beschädigung aufweisen, tauschen Sie es sofort aus.
- Trennen Sie alle Stromverbindungen, bevor Sie Arbeiten im Bereich der Stromversorgung vornehmen, sofern dies nicht für eine Wartungsprozedur anders verlangt wird.
- Gehen Sie vorsichtig vor, wenn Sie an Hotswap-fähigen Wireless Controller-Komponenten (Stromversorgungen oder Lüftern) Servicearbeiten durchführen. Rotierende Lüfter können ernsthafte Verletzungen verursachen.
- Dieses Gerät ist möglicherweise über mehr als ein Netzkabel angeschlossen. Um die Gefahr eines elektrischen Schlages zu vermeiden, sollten Sie vor Durchführung von Servicearbeiten alle Netzkabel trennen. Falls eines der Stromversorgungsmodule ausfällt, kann es ausgetauscht werden, ohne die Stromversorgung zum Wireless Controller zu unterbrechen. Bei dieser Prozedur ist jedoch mit Vorsicht vorzugehen. Das Modul kann extrem heiß sein. Tragen Sie Handschuhe, um Verbrennungen zu vermeiden.
- Bei unsachgemäßem Austausch der Lithium-Batterie besteht Explosionsgefahr. Die Lithium-Batterie darf nur durch identische oder vom Händler empfohlene Typen ersetzt werden.
- Achten Sie bei Lithium-Batterien auf die ordnungsgemäße Entsorgung.
- Versuchen Sie niemals, ohne Hilfe schwere Gegenstände zu heben.

Vorsichtshinweise

- Überprüfen Sie die für die Ausrüstung festgelegte Nennspannung (Bedienungsanleitung und Typenschild). Diese Ausrüstung arbeitet mit Hochspannung, die mit der Gefahr eines elektrischen Schlages verbunden ist. Gehen Sie mit großer Vorsicht vor, wenn Sie bei eingeschaltetem System Hochspannungen messen oder Karten, Schalttafeln und Baugruppen warten.
- Verwenden Sie nur Werkzeuge und Ausrüstung in einwandfreiem Zustand. Verwenden Sie keine Ausrüstung mit sichtbaren Beschädigungen.
- Tragen Sie bei Arbeiten an Hardwarekomponenten ein Armband, um elektrostatisch gefährdete Bauelemente (EGB) vor Beschädigungen zu schützen.
- Verlegen Sie Leitungen so, dass sie keine Unfallquelle (Stolpergefahr) bilden und nicht beschädigt werden.

Consignes De Sécurité

Dangers

- Si le cordon de raccordement au secteur est endommagé, remplacez-le immédiatement.
- Remplacez sans délai les équipements de sécurité endommagés (caches, étiquettes et conducteurs de protection).
- Utilisez uniquement les accessoires d'origine ou les modules agréés spécifiques au système. Dans le cas contraire, vous risquez d'endommager l'installation ou d'enfreindre les consignes en matière de sécurité et de compatibilité électromagnétique.
- Seul le personnel de service Extreme Networks est autorisé à maintenir/réparer le système.

Avertissements

- Cet appareil ne doit pas être connecté à un segment de LAN à l'aide d'un câblage extérieur.
- Vérifiez que tous les câbles fonctionnent correctement pour éviter une contrainte excessive.
- Si l'adaptateur d'alimentation présente des dommages, remplacez-le immédiatement.
- Coupez toujours l'alimentation avant de travailler sur les alimentations électriques, sauf si la procédure de maintenance mentionne le contraire.
- Prenez toutes les précautions nécessaires lors de l'entretien/réparations des modules du Wireless Controller pouvant être branchés à chaud : alimentations électriques ou ventilateurs. Les ventilateurs rotatifs peuvent provoquer des blessures graves.
- Cette unité peut avoir plusieurs cordons d'alimentation. Pour éviter tout choc électrique, débranchez tous les cordons d'alimentation avant de procéder à la maintenance. En cas de panne d'un des modules d'alimentation, le module défectueux peut être changé sans éteindre le Wireless Controller. Toutefois, ce remplacement doit être effectué avec précautions. Portez des gants pour éviter de toucher le module qui peut être très chaud.
- Le remplacement non conforme de la batterie au lithium peut provoquer une explosion. Remplacez la batterie au lithium par un modèle identique ou par un modèle recommandé par le revendeur.
- Sa mise au rebut doit être conforme aux prescriptions en vigueur.
- N'essayez jamais de soulever des objets qui risquent d'être trop lourds pour vous.

Précautions

- Contrôlez la tension nominale paramétrée sur l'installation (voir le mode d'emploi et la plaque signalétique). Des tensions élevées pouvant entraîner des chocs électriques sont utilisées dans cet équipement. Lorsque le système est sous tension, prenez toutes les précautions nécessaires lors de la mesure des hautes tensions et de l'entretien/réparation des cartes, des panneaux, des plaques.
- N'utilisez que des appareils et des outils en parfait état. Ne mettez jamais en service des appareils présentant des dommages visibles.
- Pour protéger les dispositifs sensibles à l'électricité statique, portez un bracelet antistatique lors du travail sur le matériel.
- Acheminez les câbles de manière à ce qu'ils ne puissent pas être endommagés et qu'ils ne constituent pas une source de danger (par exemple, en provoquant la chute de personnes).

Providing Feedback to Us

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 about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **GTAC (Global Technical Assistance Center) for Immediate Support**
 - **Phone:** 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
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **Extreme Portal** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **The Hub** — A forum for Extreme 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.

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

Extreme Networks Documentation

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

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

1 About This Guide

Who Should Use This Guide How to Use This Guide

This guide describes how to install, configure, and manage the Extreme Networks ExtremeWireless software. This guide is also available as an online help system.

To access the online help, click **Help** in the ExtremeWireless Assistant top menu bar.

Who Should Use This Guide

This guide is a reference for system administrators who install and manage the ExtremeWireless system.

Any administrator performing tasks described in this guide must have an account with administrative privileges.

How to Use This Guide

To locate information about various subjects in this guide, refer to the following table.

For...	Refer to...
An overview of the product, its features and functionality.	Overview of the ExtremeWireless Solution on page 14
Information about how to perform the installation, first time setup and configuration of the controller, as well as configuring the data ports and defining routing.	Configuring the ExtremeWireless Appliance on page 31
Information on how to install the ExtremeWireless AP, how it discovers and registers with the controller, and how to view and modify radio configuration.	Configuring the ExtremeWireless APs on page 101
An overview of topologies and provides detailed information about how to configure them.	Configuring Topologies on page 262
An overview of roles and provides detailed information about how to configure them.	Configuring Roles on page 284
An overview of <u>WLAN (Wireless Local Area Network)</u> services and provides detailed information about how to configure them.	Configuring WLAN Services on page 318
An overview of Virtual Network Services (VNS), provides detailed instructions in how to configure a VNS, either using the Wizards or by manually creating the component parts of a VNS.	Configuring a VNS on page 390
Information about configuring <u>CoS (Class of Service)</u> which are a configuration entity containing QoS Marking (802.1p and ToS/DSCP), Inbound/Outbound Rate Limiting and Transmit Queue Assignments.	Configuring Classes of Service on page 487

For...	Refer to...
Information about configuring Sites which is a mechanism for grouping APs and refers to specific Roles, Classes of Service (CoS) and RADIUS servers that are grouped to form a single configuration.	Configuring Sites on page 494
An overview of Mesh networks and provides detailed information about how to create a Mesh network.	Working with a Mesh Network on page 502
An overview of a Wireless Distribution System (WDS) network configuration and provides detailed information about how to create a Mesh network.	Working with a Wireless Distribution System on page 518
Information on how to set up the features that maintain service availability in the event of a controller failover.	Availability and Session Availability on page 537
Information on how to set up the mobility domain that provides mobility for a wireless device user when the user roams from one ExtremeWireless AP to another in the mobility domain.	Configuring Mobility on page 555
Information on how to use the ExtremeWireless AP features with third-party wireless access points.	Working with Third-party APs on page 561
Information on the security tool that scans for, detects, provides countermeasures, and reports on rogue APs.	Working with ExtremeWireless Radar on page 563
Information on the various reports and displays available in the system.	Working with Reports and Statistics on page 621
Information on system administration activities, such as performing ExtremeWireless AP client management, defining management users, configuring the network time, and configuring Web session timeouts.	Performing System Administration on page 669
Information on how to view and interpret the logs, traces, audits and <i>DHCP (Dynamic Host Configuration Protocol)</i> messages.	Logs, Traces, Audits and DHCP Messages on page 676
Information on how to configure GuestPortal accounts.	Working with GuestPortal Administration on page 690
A list of terms and definitions for the ExtremeWireless Appliance and the ExtremeWireless AP as well as standard industry terms used in this guide.	Glossary terms are displayed as links in the text. Hover over a glossary term to display the definition, or click the link to go to the Glossary.
Regulatory information for the ExtremeWireless Appliances and the ExtremeWireless APs.	Regulatory Information on page 705
The default GuestPortal ticket page source code.	Default GuestPortal Ticket Page on page 706

2 Overview of the ExtremeWireless Solution

Introduction

Conventional Wireless LANs

Elements of the ExtremeWireless Solution

ExtremeWireless and Your Network

ExtremeWireless Appliance Product Family

Introduction

The next generation of wireless networking devices provides a truly scalable *WLAN (Wireless Local Area Network)* solution. ExtremeWireless Access Points (APs, wireless APs) are fit access points controlled through a sophisticated network device, the controller. This solution provides the security and manageability required by enterprises and service providers for huge industrial wireless networks.

The ExtremeWireless system is a highly scalable Wireless Local Area Network (WLAN) solution. Based on a third generation WLAN topology, the ExtremeWireless system makes wireless practical for service providers as well as medium and large-scale enterprises.

The ExtremeWireless controller provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11 standard. The system is intended for enterprise networks operating on multiple floors in more than one building, and is ideal for public environments, such as airports and convention centers that require multiple access points.

This chapter provides an overview of the fundamental principles of the ExtremeWireless System.

The ExtremeWireless Appliance

The ExtremeWireless Appliance is a network device designed to integrate with an existing wired Local Area Network (LAN). The rack-mountable controller provides centralized management, network access, and routing to wireless devices that use Wireless APs to access the network. It can also be configured to handle data traffic from third-party access points.

The controller provides the following functionality:

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

Conventional Wireless LANs

Wireless communication between multiple computers requires that each computer be equipped with a receiver/transmitter—a *WLAN* Network Interface Card (NIC)—capable of exchanging digital information over a common radio frequency. This is called an ad hoc network configuration. An ad hoc network configuration allows wireless devices to communicate together. This setup is defined as an independent basic service set (IBSS).

An alternative to the ad hoc configuration is the use of an access point. This may be a dedicated hardware bridge or a computer running special software. Computers and other wireless devices communicate with each other through this access point. The 802.11 standard defines access point communications as devices that allow wireless devices to communicate with a distribution system. This setup is defined as a basic service set (BSS) or infrastructure network.

To allow the wireless devices to communicate with computers on a wired network, the access points must be connected to the wired network providing access to the networked computers. This topology is called bridging. With bridging, security and management scalability is often a concern.

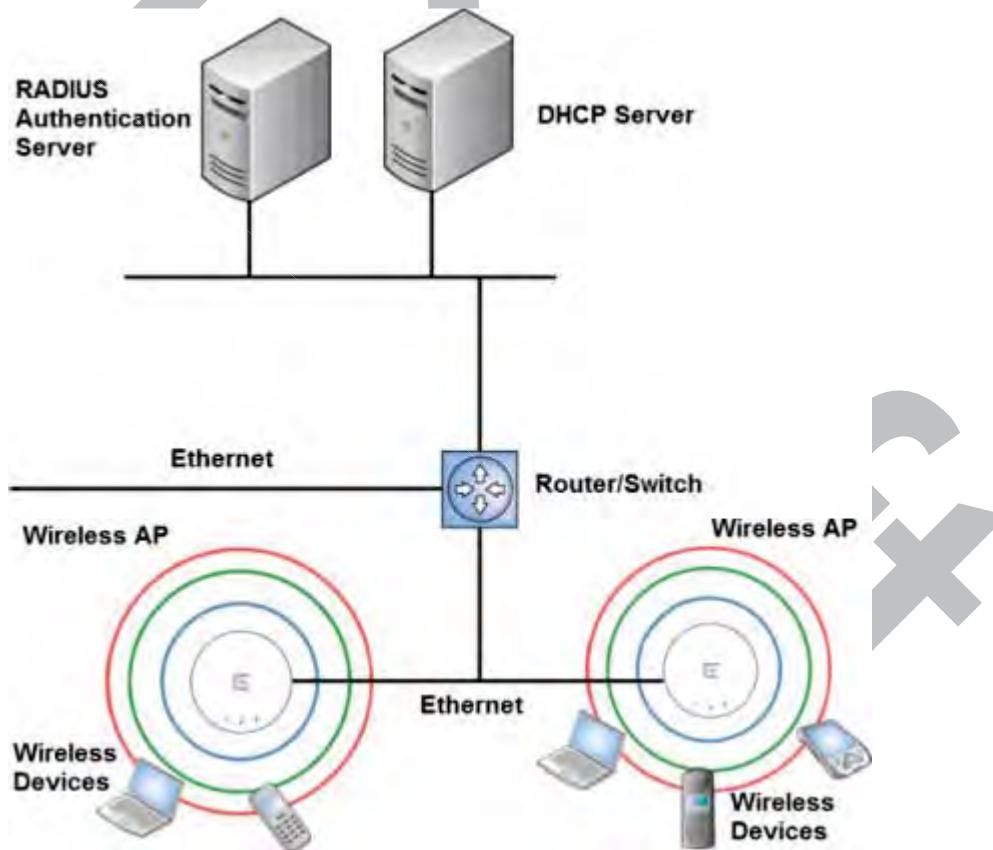


Figure 1: Standard Wireless Network Solution Example

The wireless devices and the wired networks communicate with each other using standard networking protocols and addressing schemes. Most commonly, Internet Protocol (IP) addressing is used.

Elements of the ExtremeWireless Solution

The ExtremeWireless solution consists of two devices:

- ExtremeWireless Appliance
- ExtremeWireless AP

This architecture allows a single controller to control many APs, making the administration and management of large networks much easier.

There can be several controllers in the network, each with a set of registered APs. The controllers can also act as backups to each other, providing stable network availability.

In addition to the controllers and APs, the solution requires three other components, all of which are standard for enterprise and service provider networks:

- RADIUS Server (Remote Access Dial-In User Service) or other authentication server
- *DHCP (Dynamic Host Configuration Protocol) Server* (Dynamic Host Configuration Protocol). If you do not have a DHCP Server on your network, you can enable the local DHCP Server on the controller. The local DHCP Server is useful as a general purpose DHCP Server for small subnets. For more information, see [Setting Up the Data Ports](#) on page 51.
- SLP (Service Location Protocol)

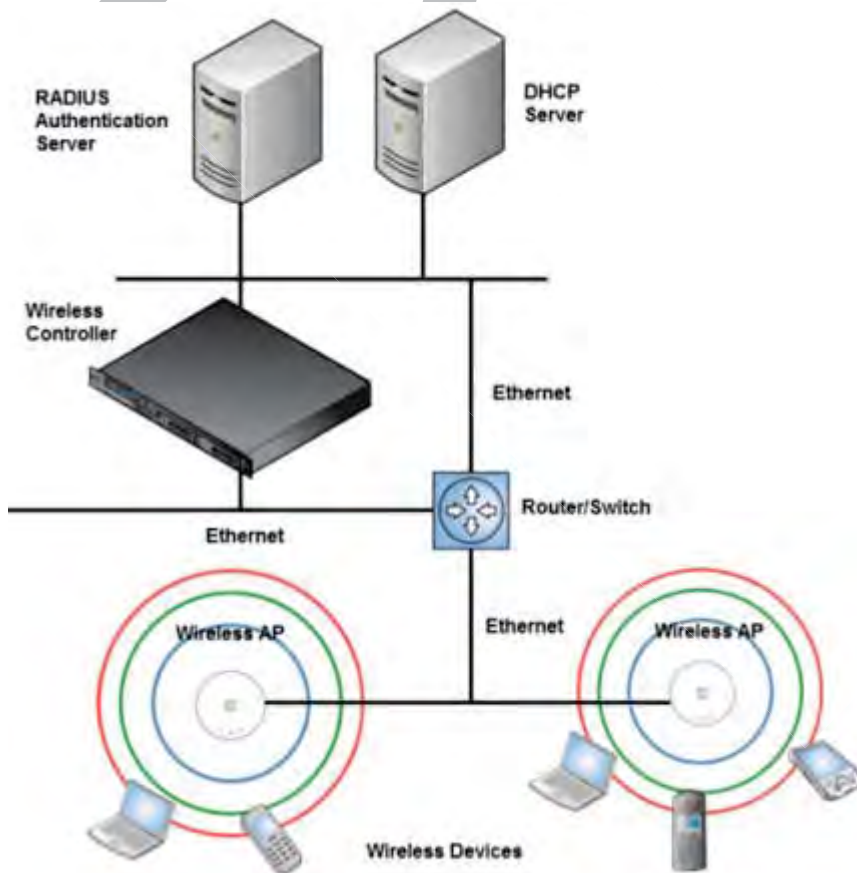


Figure 2: ExtremeWireless Appliance Solution

As illustrated in [ExtremeWireless Appliance Solution](#), the ExtremeWireless Appliance appears to the existing network as if it were an access point, but in fact one controller controls many APs. The controller has built-in capabilities to recognize and manage the APs. The controller:

- Activates the APs
- Enables APs to receive wireless traffic from wireless devices
- Processes the data traffic from the APs
- Forwards or routes the processed data traffic out to the network
- Authenticates requests and applies access roles

Simplifying the APs makes them cost-effective, easy to manage, and easy to deploy. Putting control on an intelligent centralized controller enables:

- Centralized configuration, management, reporting, and maintenance
- High security
- Flexibility to suit enterprise
- Scalable and resilient deployments with a few controllers controlling hundreds of APs

The ExtremeWireless system:

- Scales up to Enterprise capacity — ExtremeWireless Appliances are scalable:
 - C5215 — Up to 1000 APs, 2000 APs in Controller availability mode
 - C5210 — Up to 1000 APs, 2000 APs in Controller availability mode
 - C5110 — Up to 525 APs, 1050 APs in Controller availability mode
 - C4110 — Up to 250 APs, 500 APs in Controller availability mode
 - C25 — Up to 50 APs, 100 APs in Controller availability mode
 - C35 — Up to 125 APs, 250 APs in Controller availability mode
 - V2110 (Small Profile) — Up to 50 APs, 100 APs in Controller availability mode
 - V2110 (Medium Profile) — Up to 250 APs, 500 APs in Controller availability mode
 - V2110 (Large Profile) — Up to 525 APs, 1050 APs in Controller availability mode
 - In turn, each wireless AP can handle a mixture of secure and non-secure clients. AP per radio support is up to 200 clients, of which 127 are clients with security. With additional controllers, the number of wireless devices the solution can support can reach into the thousands.
- Integrates with existing network — A controller can be added to an existing enterprise network as a new network device, greatly enhancing its capability without interfering with existing functionality. Integration of the controllers and APs does not require any re-configuration of the existing infrastructure (for example, VLAN (Virtual LAN)s).
- Integrates with the Extreme Networks Extreme Management Center Suite of products. For more information, see [Extreme Networks Extreme Management Center Integration](#) on page 18.

Plug-in applications include:

- Automated Security Manager
- Inventory Manager
- NAC Manager
- Role Control Console
- Policy Manager
- Offers centralized management and control — An administrator accesses the controller in its centralized location to monitor and administer the entire wireless network. From the controller the administrator can recognize, configure, and manage the APs and distribute new software releases.
- Provides easy deployment of APs — The initial configuration of the APs on the centralized controller can be done with an automatic “discovery” technique.

- Provides security via user authentication — Uses existing authentication (AAA) servers to authenticate and authorize users.
- Provides security via filters and privileges — Uses virtual networking techniques to create separate virtual networks with defined authentication and billing services, access roles, and privileges.
- Supports seamless mobility and roaming — Supports seamless roaming of a wireless device from one wireless AP to another on the same controller or on a different controller.
- Integrates third-party access points — Uses a combination of network routing and authentication techniques.
- Prevents rogue devices — Unauthorized access points are detected and identified as either harmless or dangerous rogue APs.
- Provides accounting services — Logs wireless user sessions, user group activity, and other activity reporting, enabling the generation of consolidated billing records.
- Offers troubleshooting capability — Logs system and session activity and provides reports to aid in troubleshooting analysis.
- Offers dynamic RF management — Automatically selects channels and adjusts Radio Frequency (RF) signal propagation and power levels without user intervention.

Extreme Networks Extreme Management Center Integration

The ExtremeWireless solution now integrates with the Extreme Management Center suite of products, a collection of tools to help you manage networks. Its client/server architecture lets you manage your network from a single workstation or, for networks of greater complexity, from one or more client workstations. It is designed to facilitate specific network management tasks while sharing data and providing common controls and a consistent user interface.

The Extreme Management Center is a family of products comprising the Extreme Management Center Console and a suite of plug-in applications, including:

- Automated Security Manager — Automated Security Manager is a unique threat response solution that translates security intelligence into security enforcement. It provides sophisticated identification and management of threats and vulnerabilities. For information on how the ExtremeWireless solution integrates with the Automated Security Manager application, see the *Maintenance Guide*.
- Inventory Manager — Inventory Manager is a tool for efficiently documenting and updating the details of the ever-changing network. For information on how the ExtremeWireless solution integrates with the Automated Security Manager application, see the *Maintenance Guide*.
- NAC Manager — NAC Manager is a leading-edge NAC solution to ensure only the right users have access to the right information from the right place at the right time. The Extreme Networks NAC solution performs multi-user, multi-method authentication, vulnerability assessment and assisted remediation. For information on how the ExtremeWireless solution integrates with the Extreme Networks NAC solution, see [NAC Integration with the Wireless WLAN](#) on page 24.
- Policy Manager — Policy Manager recognizes the ExtremeWireless suite as role capable devices that accept partial configuration from Policy Manager. Currently this integration is partial in the sense that Extreme Management Center is unable to create WLAN services directly; The WLAN services need to be directly provisioned on the controller and are represented to Policy Manager as logical ports.

The ExtremeWireless Appliance allows Policy Manager to:

- Attach Topologies (assign VLAN to port) to the ExtremeWireless Appliance physical ports (Console).
- Attach role to the logical ports (WLAN Service/SSID),
- Assign a Default Role/Role to a WLAN Service, thus creating the VNS.
- Perform authentication operations which can then reference defined roles for station-specific role enforcement.

This can be seen as a three-step process:

- 1 Deploy the controller and perform local configuration
 - The ExtremeWireless Appliance ships with a default SSID, attached by default to all AP radios, when enabled.
 - Use the basic installation wizard to complete the ExtremeWireless Appliance configuration.
- 2 Use Policy Manager to:
 - Push the VLAN list to the ExtremeWireless Appliance (Topologies)
 - Attach VLANs to ExtremeWireless Appliance physical ports (Console - Complete Topology definition)
 - Push RADIUS server configuration to the ExtremeWireless Appliance
 - Push role definitions to the ExtremeWireless Appliance
 - Attach the default role to create a VNS
- 3 Fine tune controller settings. For example, configuring filtering at APs and ExtremeWireless Appliance for a bridged at controller or routed topologies and associated VNSs.



Note

Complete information about integration with Policy Manager is outside the scope of this document.

ExtremeWireless and Your Network

This section is a summary of the components of the ExtremeWireless solution on your enterprise network. The following are described in detail in this guide, unless otherwise stated:

- ExtremeWireless Appliance — A rack-mountable network device or virtual appliance that provides centralized control over all access points and manages the network assignment of wireless device clients associating through access points.
- Wireless AP — A wireless LAN fit access point that communicates with a controller.
- RADIUS Server (Remote Access Dial-In User Service) (RFC2865), or other authentication server — An authentication server that assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users in either 802.1x or Captive Portal security modes. The RADIUS Server system can be set up for certain standard attributes, such as filter ID, and for the Vendor Specific Attributes (VSAs). In addition, RADIUS Disconnect (RFC3576) which permits dynamic adjustment of user role (user disconnect) is supported.
- DHCP Server (Dynamic Host Configuration Protocol) (RFC2131) — A server that assigns dynamically IP addresses, gateways, and subnet masks. IP address assignment for clients can be done by the DHCP server internal to the controller, or by existing servers using DHCP relay. It is also used by the APs to discover the location of the controller during the initial registration process using Options 43, 60, and Option 78. Options 43 and 60 specify the vendor class identifier (VCI) and vendor specific

information. Option 78 specifies the location of one or more SLP Directory Agents. For SLP, DHCP should have Option 78 enabled.

- Service Location Protocol (SLP) (SLP RFC2608) — Client applications are User Agents and services that are advertised by a Service Agent. In larger installations, a Directory Agent collects information from Service Agents and creates a central repository. The Extreme Networks solution relies on registering “Extreme Networks” as an SLP Service Agent.
- Domain Name Server (DNS) — A server used as an alternate mechanism (if present on the enterprise network) for the automatic discovery process. Controller, Access Points and Convergence Software relies on the DNS for Layer 3 deployments and for static configuration of the APs. The controller can be registered in DNS, to provide DNS assisted AP discovery. In addition, DNS can also be used for resolving RADIUS server hostnames.
- Web Authentication Server — A server that can be used for external Captive Portal and external authentication. The controller has an internal Captive portal presentation page, which allows web authentication (web redirection) to take place without the need for an external Captive Portal server.
- RADIUS Accounting Server (Remote Access Dial-In User Service) (RFC2866) — A server that is required if RADIUS Accounting is enabled.
- SNMP (Simple Network Management Protocol) — A Manager Server that is required if forwarding SNMP messages is enabled.
- Network Infrastructure — The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple controllers for the following features to operate successfully:
 - Availability
 - Mobility
 - ExtremeWireless Radar for detection of rogue access points

Some features also require the definition of static routes.

- Web Browser — A browser provides access to the controller Management user interface to configure the ExtremeWireless system.
- SSH Enabled Device — A device that supports Secure Shell (SSH) is used for remote (IP) shell access to the system.
- Zone Integrity — The Zone integrity server enhances network security by ensuring clients accessing your network are compliant with your security roles before gaining access. Zone Integrity Release 5 is supported.
- (Optional) Online Signup Server — For use with Hotspot Networks.

Network Traffic Flow

Figure 3 illustrates a simple configuration with a single controller and two APs, each supporting a wireless device. A RADIUS server on the network provides authentication, and a *DHCP* server is used by the APs to discover the location of the controller during the initial registration process. Network inter-connectivity is provided by the infrastructure routing and switching devices.

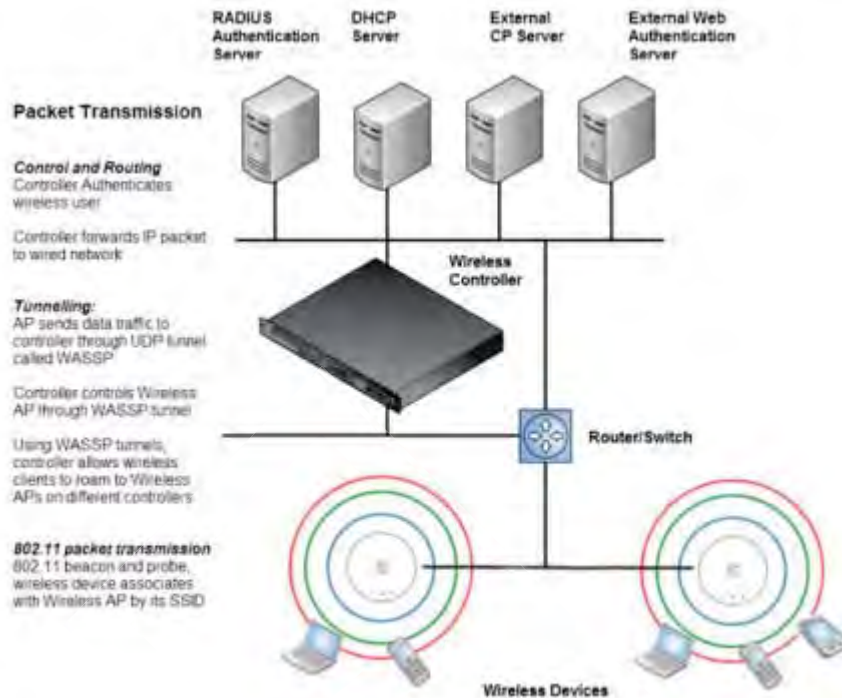


Figure 3: Traffic Flow Diagram

Each wireless device sends IP packets in the 802.11 standard to the AP. The AP uses a UDP (User Datagram Protocol) based tunnelling protocol. In tunneled mode of operation, it encapsulates the packets and forwards them to the controller. The controller decapsulates the packets and routes these to destinations on the network. In a typical configuration, access points can be configured to locally bridge traffic (to a configured VLAN) directly at their network point of attachment.

The controller functions like a standard L3 router or L2 switch. It is configured to route the network traffic associated with wireless connected users. The controller can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred or available.

Network Security

The Extreme Networks ExtremeWireless system provides features and functionality to control network access. These are based on standard wireless network security practices.

Current wireless network security methods provide protection. These methods include:

- Shared Key authentication that relies on Wired Equivalent Privacy (WEP) keys
- Open System that relies on Service Set Identifiers (SSIDs)
- 802.1x that is compliant with Wi-Fi Protected Access (WPA)
- Captive Portal based on Secure Sockets Layer (SSL) protocol

The Extreme Networks ExtremeWireless system provides the centralized mechanism by which the corresponding security parameters are configured for a group of users.

- Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks defined in the 802.11b standard

- Wi-Fi Protected Access version 1 (WPA1™) with Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access version 2 (WPA2™) with Advanced Encryption Standard (AES) and Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP)

Authentication

The controller relies on a RADIUS server, or authentication server, on the enterprise network to provide the authentication information (whether the user is to be allowed or denied access to the network). A RADIUS client is implemented to interact with infrastructure RADIUS servers.

The controller provides authentication using:

- Captive Portal — a browser-based mechanism that forces users to a Web page
- RADIUS (using IEEE 802.1x)

The 802.1x mechanism is a standard for authentication developed within the 802.11 standard. This mechanism is implemented at the wireless port, blocking all data traffic between the wireless device and the network until authentication is complete. Authentication by 802.1x standard uses Extensible Authentication Protocol (EAP) for the message exchange between the controller and the RADIUS server.

When 802.1x is used for authentication, the controller provides the capability to dynamically assign per-wireless-device WEP keys (called per session WEP keys in 802.11). In the case of WPA, the controller is not involved in key assignment. Instead, the controller is involved in the information exchange between RADIUS server and the user's wireless device to negotiate the appropriate set of keys. With WPA2 the material exchange produces a Pairwise Master Key which is used by the AP and the user to derive their temporal keys. (The keys change over time.)

The Extreme Networks ExtremeWireless solution provide a RADIUS redundancy feature that enables you to define a failover RADIUS server in the event that the active RADIUS server becomes unresponsive.

Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques.

Extreme Networks ExtremeWireless supports the Wired Equivalent Privacy (WEP) standard common to conventional access points.

It also provides Wi-Fi Protected Access version 1 (WPA v.1) encryption, based on Pairwise Master Key (PMK) and Temporal Key Integrity Protocol (TKIP). The most secure encryption mechanism is WPA version 2, using Advanced Encryption Standard (AES).

Virtual Network Services

Virtual Network Services (VNS) provide a versatile method of mapping wireless networks to the topology of an existing wired network.

In releases prior to V7.0, a VNS was a collection of operational entities. Starting with Release V7.0, a VNS becomes the binding of reusable components:

- *WLAN* Service components that define the radio attributes, privacy and authentication settings, and QoS attributes of the VNS
- Role components that define the topology (typically a *VLAN*), policy rules, and Class of Service applied to the traffic of a station.

Figure 4 illustrates the transition of the concept of a VNS to a binding of reusable components.

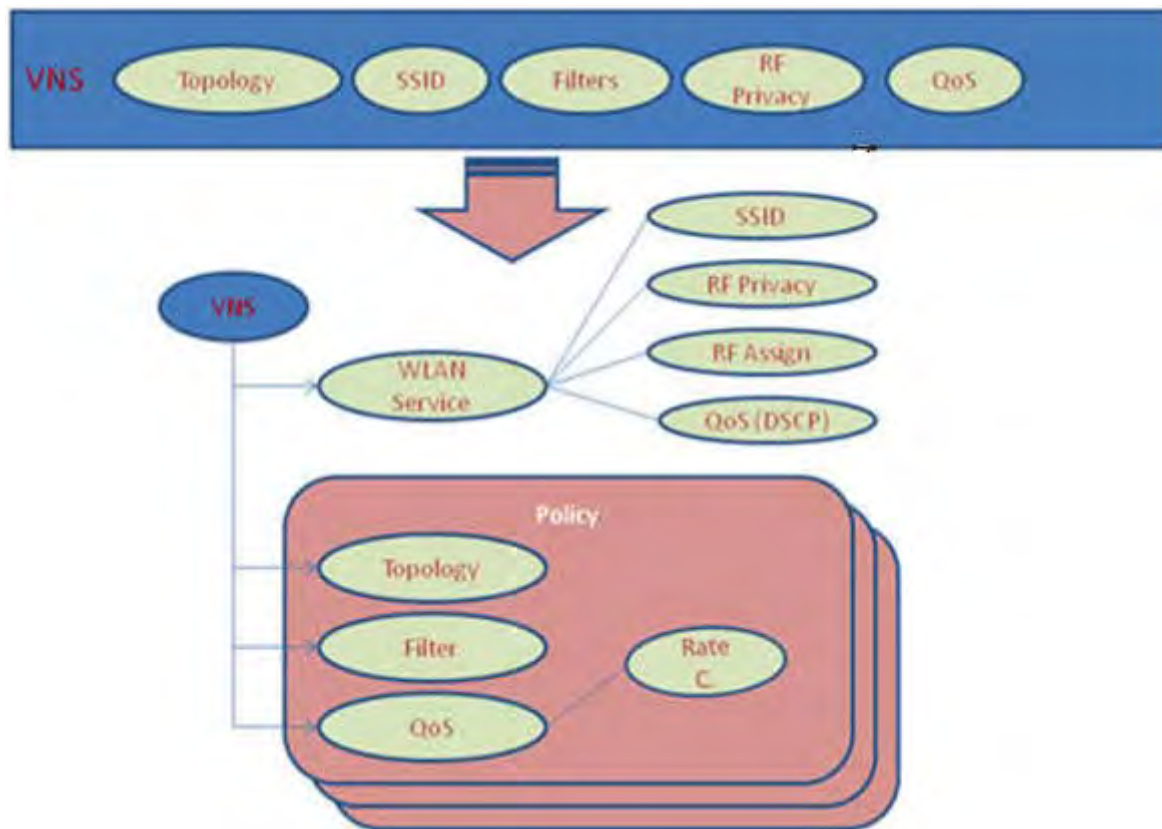


Figure 4: VNS as a Binding of Reusable Components

WLAN Service components and Role components can be configured separately and associated with a VNS when the VNS is created or modified. Alternatively, they can be configured during the process of creating a VNS.

Additionally, Roles can be created using the Extreme Networks Extreme Management Center Policy Manager or Extreme Management Center Wireless Manager and pushed to the ExtremeWireless Appliance. Role assignment ensures that the correct topology and traffic behavior are applied to a user regardless of WLAN service used or VNS assignment.

When VNS components are set up on the controller, among other things, a range of IP addresses is set aside for the controller's *DHCP* server to assign to wireless devices.

If the *OSPF (Open Shortest Path First)* routing protocol is enabled, the controller advertises the routed topologies as reachable segments to the wired network infrastructure. The controller routes traffic between the wireless devices and the wired network.

The controller also supports VLAN-bridged assignment for VNSs. This allows the controller to directly bridge the set of wireless devices associated with a WLAN service directly to a specified core VLAN.

Each controller model can support a definable number and an active number of VNSs. See [Table 3](#).

Table 3: VNS and WLAN Service Capacity

Controller Model	Max Number of Defined VNS	Max Number of Defined WLAN Services	Max Number of Active WLAN Services
C5110	256	256	128
C4110	128	128	64
C25	32	32	16
V2110 Small	32	32	16
V2110 Medium V2110-HyperV	128	128	64
V2110 Large	256	256	128
C5215	256	256	128
C5210	256	256	128
C35	32	16	32

The AP radios can be assigned to each of the configured WLAN services and, therefore, VNSs in a system. Each AP can be the subject of 16 service assignments—eight assignments per radio—which corresponds to the number of SSIDs it can support. Once a radio has all eight slots assigned, it is no longer eligible for further assignment.

The AP3912 has three additional client ports that can be assigned to a single WLAN Service. For more information, see [Assigning WLAN Services to Client Ports](#) on page 170.

NAC Integration with the Wireless WLAN

The Extreme Networks Wireless *WLAN* supports integration with a NAC (Network Admission Control) Gateway. The NAC Gateway can provide your network with authentication, registration, assessment, remediation, and access control for mobile users.

NAC Gateway integration with Wireless WLAN supports SSID VNSs when used in conjunction with MAC-based external captive portal authentication.

[Figure 5](#) depicts the topology and workflow relationship between Wireless WLAN that is configured for external captive portal and a NAC Gateway. With this configuration, the NAC Gateway acts like a RADIUS proxy server. An alternative is to configure the NAC Gateway to perform MAC-based authentication itself, using its own database of MAC addresses and permissions. For more information, see [Creating a NAC VNS Using the VNS Wizard](#) on page 426.

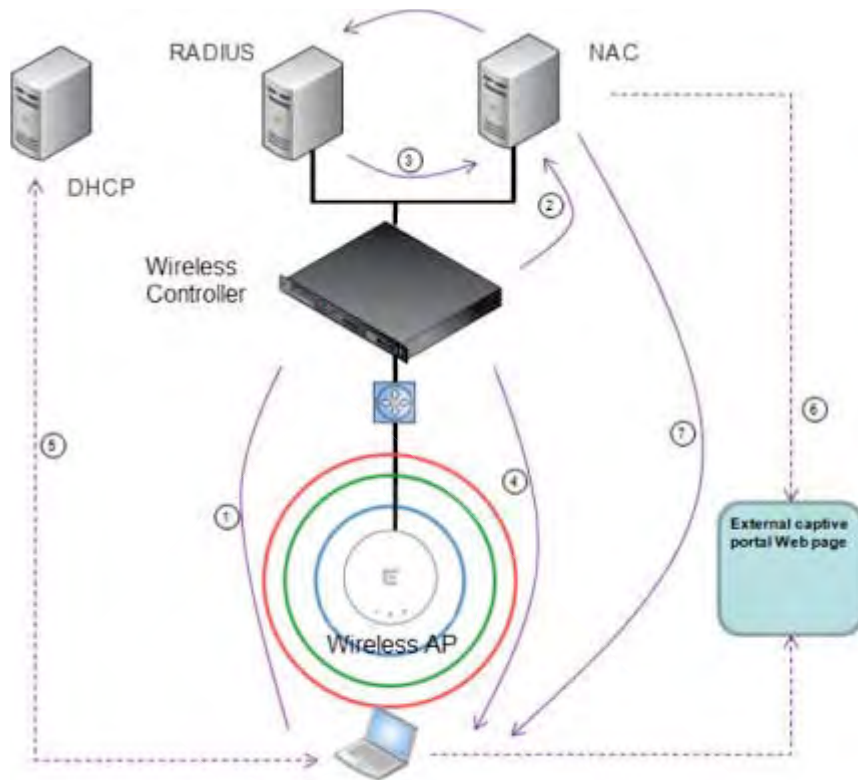


Figure 5: WLAN and NAC Integration with External Captive Portal Authentication

- 1 The client laptop connects to the AP.

The AP determines that authentication is required, and sends an association request to the appliance.

- 2 The appliance forwards to the NAC Gateway an access-request message for the client laptop, which is identified by its MAC address.

The NAC Gateway forwards the access-request to the RADIUS server. The NAC Gateway acts like a RADIUS proxy server.

- 3 The RADIUS server evaluates the access-request and sends an AccessAccept message back to the NAC.



Note

RADIUS servers with captive portal and EAP authentication can be tested for connectivity using the `radtest` command. For more information, see the ExtremeWireless CLI Guide.

The NAC receives the access-accept packet. Using its local database, the NAC determines the correct role to apply to this client laptop and updates the access-accept packet with the role assignment. The updated AccessAccept message is forwarded to the appliance and AP.

- 4 The appliance and the AP apply role against the client laptop accordingly. The appliance assigns a set of filters to the client laptop's session and the AP allows the client laptop access to the network.
- 5 The client laptop interacts with a DHCP server to obtain an IP address.
- 6 Eventually the client laptop uses its web browser to access a website.
 - The appliance determines that the target website is blocked and that the client laptop still requires authentication.

- The appliance sends an HTTP redirect to the client laptop's browser. The redirect sends the browser to the web server on the NAC Gateway.
 - The NAC displays an appropriate web page in the client laptop's browser. The contents of the page depend on the current role assignment (enterprise, remediation, assessing, quarantine, or unregistered) for the MAC address.
- 7 When the NAC determines that the client laptop is ready for a different role assignment, it sends a 'disconnect message' (RFC 3576) to the appliance.

When the appliance receives the 'disconnect message' sent by the NAC, the appliance terminates the session for the client laptop.

The appliance forwards the command to terminate the client laptop's session to the AP, which disconnects the client laptop.

VNS Components

The distinct constituent high-level configurable umbrella elements of a VNS are:

- **Topology**
- **Role**
- **Classes of Service**
- **WLAN Service**

Topology

Topologies represent the networks with which the controller and its APs interact. The main configurable attributes of a topology are:

- Name - a string of alphanumeric characters designated by the administrator.
- VLAN ID - the VLAN identifier as specified in the IEEE 802.1Q definition.
- VLAN tagging options.
- Port of presence for the topology on the controller. (This attribute is not required for Routed and Bridged at AP topologies.)
- Interface. This attribute is the IP (L3) address assigned to the controller on the network described by the topology. (Optional.)
- Type. This attribute describes how traffic is forwarded on the topology. Options are:
 - "Physical" - the topology is the native topology of a data plane and it represents the actual Ethernet ports
 - "Management" - the native topology of the controller management port
 - "Routed" - the controller is the routing gateway for the routed topology.
 - "Bridged at Controller" - the user traffic is bridged (in the L2 sense) between wireless clients and the core network infrastructure.
 - "Bridged at AP" - the user traffic is bridged locally at the AP without being redirected to the controller
- Exception Filters. Specifies which traffic has access to the controller from the wireless clients or the infrastructure network.
- Certificates.

- Multicast filters. Defines the multicast groups that are allowed on a specific topology segment.
- For information about Topology groups, see [Creating a Topology Group](#) on page 270.

Role

A Role is a collection of attributes and rules that determine actions taken user traffic accesses the wired network through the *WLAN* service (associated to the WLAN Service's SSID). Depending upon its type, a VNS can have between one and three Authorization Roles associated with it:

- 1 Default non-authorized role — This is a mandatory role that covers all traffic from stations that have not authenticated. At the administrator's discretion the default non-authorized role can be applied to the traffic of authenticated stations as well.
- 2 Default authorized role — This is a mandatory role that applies to the traffic of authenticated stations for which no other role was explicitly specified. It can be the same as the default non-authorized role.
- 3 Third-party AP role — This role applies to the list of MAC addresses corresponding to the wired interfaces of third party APs specifically defined by the administrator to be providing the RF access as an AP WLAN Service. This role is only relevant when applied to third party AP WLAN Services.

Classes of Service

In general, *CoS (Class of Service)* 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 station or port assigned to a specific role is permitted. The CoS defines actions to be taken when rate limits are exceeded.

All incoming packets may follow these steps to determine a CoS:

- Classification - identifies the first matching rule that defines a CoS.
- Marking - modifies the L2 802.1p and/or L3 ToS based on CoS definition.
- Rate limiting (drop) is set.

The system limit for the number of CoS profiles on a controller is identical to the number of roles. For example, the maximum number of CoS profiles on a C4110 is 512.

WLAN Services

A *WLAN* Service represents all the RF, authentication and QoS attributes of a wireless access service offered by the controller and its APs. A WLAN Service can be one of the following types:

- Standard — A conventional service. Only APs running ExtremeWireless software can be part of this WLAN Service. This type of service can be used as a Bridged at Controller, Bridged at AP, or Routed Topology. This type of service provides access for mobile stations. Roles can be associated with this type of WLAN service to create a VNS. Hotspot can be enabled for standard WLAN services.
- Third Party AP — A Wireless Service offered by third party APs. This type of service provides access for mobile stations. Roles can be assigned to this type of WLAN service to create a VNS.
- Dynamic Mesh and WDS (Static Mesh)— This is to configure a group of APs organized into a hierarchy for purposes of providing a Wireless Distribution Service. This type of service is in essence

a wireless trunking service rather than a service that provides access for stations. As such, this service cannot have roles attached to it.

- Remote — A service that resides on the edge (foreign) controller. Pairing a remote service with a remoteable service on the designated home controller allows you to provision centralized WLAN Services in the mobility domain. This is known as centralized mobility.

The components of a WLAN Service map to the corresponding components of a VNS in previous releases. The administrator makes an explicit choice of the type of authentication to use on the WLAN Service. If the choice of authentication option conflicts with any other authentication or privacy choices, the WLAN Service cannot be enabled.

Routing

Routing can be used on the controller to support the VNS definitions. Through the user interface you can configure routing on the controller to use one of the following routing techniques:

- Static routes — Use static routes to set the default route of a controller so that legitimate wireless device traffic can be forwarded to the default gateway.
- *OSPF* (version 2) (RFC2328) — Use OSPF to allow the controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation. Static Route definition and OSPF dynamic learning can be combined, and the precedence of a static route definition over dynamic rules can be configured by selecting or clearing the Override dynamic routes option check box.
- Next-hop routing — Use next-hop routing to specify a unique gateway to which traffic on a VNS is forwarded. Defining a next-hop for a VNS forces all the traffic in the VNS to be forwarded to the indicated network device, bypassing any routing definitions of the controller's route table.

Mobility and Roaming

In typical simple configurations, APs are set up as bridges that bridge wireless traffic to the local subnet. In bridging configurations, the user obtains an IP address from the same subnet as the AP, assuming no *VLAN* trunking functionality. If the user roams between APs on the same subnet, it is able to keep using the same IP address. However, if the user roams to another AP outside of that subnet, its IP address is no longer valid. The user's client device must recognize that the IP address it has is no longer valid and re-negotiate a new one on the new subnet. This mechanism does not mandate any action on the user. The recovery procedure is entirely client device dependent. Some clients automatically attempt to obtain a new address on roam (which affects roaming latency), while others will hold on to their IP address. This loss of IP address continuity seriously affects the client's experience in the network, because in some cases it can take minutes for a new address to be negotiated.

The Extreme Networks ExtremeWireless solution centralizes the user's network point of presence, therefore abstracting and decoupling the user's IP address assignment from that of the APs location subnet. That means that the user is able to roam across any AP without losing its own IP address, regardless of the subnet on which the serving APs are deployed.

In addition, a controller can learn about other controllers on the network and then exchange client session information. This enables a wireless device user to roam seamlessly between different APs on different controllers.

Network Availability

The Extreme Networks ExtremeWireless solution provides availability against AP outages, controller outages, and even network outages. The controller in a VLAN bridged topology can potentially allow the user to retain the IP address in a failover scenario, if the VNS/VLAN is common to both controllers. For example, availability is provided by defining a paired controller configuration by which each peer can act as the backup controller for the other's APs. APs in one controller are allowed to fail over and register with the alternate controller.

If the primary controller fails, all of its associated APs can automatically switch over to another controller that has been defined as the secondary or backup controller. If an AP reboots, the primary controller is restored if it is active. However, active APs will continue to be connected to the backup controller until the administrator releases them back to the primary home controller.

Quality of Service (QoS)

Extreme Networks ExtremeWireless solution provides advanced Quality of Service (QoS) management to provide better network traffic flow. Such techniques include:

- WMM (Wi-Fi Multimedia) — WMM is enabled per WLAN service. The controller provides centralized management of the AP features. For devices with 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. In the context of the ExtremeWireless Solution, the ToS/DSCP field is used for classification and proper class of service mapping, output queue selection, and priority tagging.
- IP ToS (Type of Service) or DSCP (Diffserv Codepoint) — The ToS/DSCP field in the IP header of a frame indicates the priority and class of service for each frame. Adaptive QoS ensures correct priority handling of client payload packets tunneled between the controller and AP by copying the IP ToS/DSCP setting from client packet to the header of the encapsulating tunnel packet.
- Rate Control — Rate Control for user traffic can also be considered as an aspect of QoS. As part of Role definition, the user can specify (default) role that includes Ingress and Egress rate control. Ingress rate control applies to traffic generated by wireless clients and Egress rate control applies to traffic targeting specific wireless clients. The bit-rates can be configured as part of globally available profiles which can be used by any particular configuration. A global default is also defined.

Quality of Service (QoS) management is also provided by:

- Assigning high priority to a WLAN service
- Adaptive QoS (automatic and all time feature)
- Support for legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic (configurable)

ExtremeWireless Appliance Product Family

The ExtremeWireless Appliance is available in the following product families:

Table 4: ExtremeWireless Product Families

ExtremeWireless Appliance Model Number	Specifications
C5110	<ul style="list-style-type: none"> • Three data ports supporting up to 525 APs • 2 fiber optic SR (10Gbps) • 1 Ethernet port GigE • One management port (Ethernet) GigE • One console port (DB9 serial) • Four USB ports – two on each front and back panel (only one port active at a time) • Redundant dual power supply unit
C5210/C5215	<ul style="list-style-type: none"> • Four data ports supporting up to 1000 APs • 2 SFP+ (10Gbps) • 2 Ethernet port GigE • One management port (Ethernet) GigE • One console port (RJ-45 serial) • Five USB ports – two on front and three on back panel (only one port active at a time) • Redundant dual power supply unit
C4110	<ul style="list-style-type: none"> • Four GigE ports supporting up to 250 APs • One management port (Ethernet) GigE • One console port (DB9 serial) • Four USB ports (only one active at a time) • Redundant dual power supply unit
C25	<ul style="list-style-type: none"> • Two GigE ports supporting up to 50 APs • One management port GigE • One console port (DB9 serial) • Two USB ports
V2110	<ul style="list-style-type: none"> • Two GigE ports or 10G fiber ports supporting up to 525 APs • One management port GigE • USB ports (only one active at a time)
C35	<ul style="list-style-type: none"> • Four GigE ports supporting up to 125 APs • One management port GigE • One console port • Two USB ports

3 Configuring the ExtremeWireless Appliance

System Configuration Overview

Logging on to the ExtremeWireless Appliance

Wireless Assistant Home Screen

Working with the Basic Installation Wizard

Configuring the ExtremeWireless Appliance for the First Time

Using a Third-party Location-based Solution

Additional Ongoing Operations of the System

System Configuration Overview

The following section provides a high-level overview of the steps involved in the initial configuration of ExtremeWireless:

- 1 Before you begin the configuration process, research the type of *WLAN (Wireless Local Area Network)* deployment that is required. For example, topology and *VLAN (Virtual LAN)* IDs, SSIDs, security requirements, and filter roles.
- 2 Prepare the network servers. Ensure that the external servers, such as *DHCP (Dynamic Host Configuration Protocol)* and RADIUS servers (if applicable) are available and appropriately configured.
- 3 Install the controller. For more information, see the documentation for your controller.
- 4 Perform the first time setup of the controller on the physical network, which includes configuring the IP addresses of the interfaces on the controller.
 - a Create a new physical topology and provide the IP address to be the relevant subnet point of attachment to the existing network.
 - b To manage the controller through the interface configured above, select the Mgmt check box on the **Interfaces** tab.
 - c Configure the data port interfaces to be on separate VLANs, matching the VLANs configured in step 3 above. Ensure also that the tagged vs. untagged state is consistent with the switch port configuration.
 - d Configure the time zone. Because changing the time zone requires restarting the controller, it is recommended that you configure the time zone during the initial installation and configuration of

the controller to avoid network interruptions. For more information, see [Configuring Network Time](#) on page 89.

- e Apply an activation key file. If an activation key is not applied, the controller functions with some features enabled in demonstration mode. Not all features are enabled in demonstration mode. For example, mobility is not enabled and cannot be used.

Caution



Whenever the licensed region changes on the ExtremeWireless Appliance, all APs are changed to Auto Channel Select to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings will be lost. Installing the new license key before upgrading will prevent the ExtremeWireless Appliance from changing the licensed region, and in addition, manually configured channel settings will be maintained. For more information, see the [ExtremeWireless Maintenance Guide](#).

- 5 Configure the controller for remote access:
 - a Set up an administration station (laptop) on subnet 192.168.10.0/24. By default, the controller's Management interface is configured with the static IP address 192.168.10.1.
 - b Configure the controller's management interface.
 - c Configure the data interfaces.
 - d Set up the controller on the network by configuring the physical data ports.
 - e Configure the routing table.
 - f Configure static routes or [OSPF \(Open Shortest Path First\)](#) parameters, if appropriate to the network.

For more information, see [Configuring the ExtremeWireless Appliance for the First Time](#) on page 45.

- 6 Configure the traffic topologies your network must support. Topologies represent the controller's points of network attachment, and therefore VLANs and port assignments need to be coordinated with the corresponding network switch ports. For more information, see [Configuring a Basic Data Port Topology](#) on page 266.
- 7 Configure roles. Roles are typically bound to topologies. Role application assigns user traffic to the corresponding network point.
 - Roles define user access rights (filtering or [ACL \(Access Control List\)](#))
 - Polices reference user's rate control profile.

For more information, see [Configuring Roles](#) on page 284.

- 8 Configure WLAN services.
 - Define SSID and privacy settings for the wireless link.
 - Select the set of APs/Radios on which the service is present.
 - Configure the method of credential authentication for wireless users (None, Internal CP, External CP, GuestPortal, 802.1x[EAP])

For more information, see [Configuring WLAN Services](#) on page 318.

- 9 Create the VNSs.

A VNS binds a WLAN Service to a Role that will be used for default assignment upon a user's network attachment.

You can create topologies, roles, and WLAN services first, before configuring a VNS, or you can select one of the wizards (such as the VNS wizard), or you can simply select to create new VNS.

The VNS page then allows for in-place creation and definition of any dependency it may require, such as:

- Creating a new WLAN Service
- Creating a new role
- Creating a new class of service (within a role)
- Creating a new topology (within a role)
- Creating new rate controls, and other Class of Service parameters

The default shipping configuration does not ship any pre-configured WLAN Services, VNSs, or Roles.

10 Install, register, and assign APs to the VNS.

- Confirm the latest firmware version is loaded. For more information, see [Performing AP Software Maintenance](#) on page 235.
- Deploy APs to their corresponding network locations.
- If applicable, configure a default AP template for common radio assignment, whereby APs automatically receive complete configuration. For typical deployments where all APs are to have the same configuration, this feature will expedite deployment, as an AP will automatically receive full configuration (including VNS-related assignments) upon initial registration with the controller. If applicable, modify the properties or settings of the APs. For more information, see [Configuring the ExtremeWireless APs](#) on page 101.
- Connect the APs to the controller.
- Once the APs are powered on, they automatically begin the Discovery process of the controller, based on factors that include:
 - Their Registration mode (on the **AP Registration** screen)
 - The enterprise network services that will support the discovery process

Logging on to the ExtremeWireless Appliance

- 1 Start your Web browser (Internet Explorer version 11 or later, FireFox, or Chrome).
See the Release Notes for the supported web browsers.

- 2 In the browser address bar, type the following, using the IP address of your controller:

`https://192.168.10.1:5825`

This launches the Wireless Assistant. The login screen displays.



- 3 Type your user name and password and click **Login**. The **Wireless Assistant Home** screen displays.



Note

The default User Name is "admin". The default Password is "abc123".

Wireless Assistant Home Screen

The **Wireless Assistant Home** screen provides real-time status information on the current state of the wireless network. Information is grouped under multiple functional areas, and the Wireless Assistant Home Screen provides a graphical representation of information related to the active APs (such as the number of wired packets, stations, and total APs). Navigate the Wireless Assistant using the top menu bar tabs.

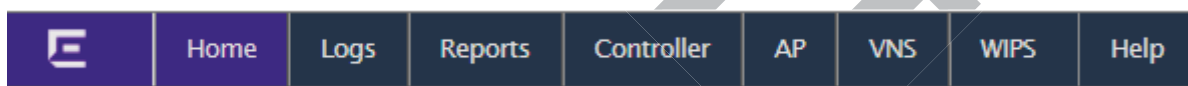


Figure 6: Wireless Assistant Top Menu Bar

The bottom status bar displays the type and description of the current wireless controller, user and admin login status, flash status, software version and the number of admin users currently logged into the controller.



Figure 7: Wireless Assistant Home Screen

Table 5 describes the panes on the Wireless Assistant Home Screen.

Table 5: Wireless Assistant Home Screen

Home Screen Heading	Description
Network Status	<p>Includes real-time totals for the following components. Click the number displayed to display additional information, such as name, serial number, and IP address.</p> <ul style="list-style-type: none"> Local APs - total number of active or inactive local configured APs. Foreign APs - total number of active or inactive foreign configured APs. Availability pair must be configured to display additional information. Pending APs - total APs pending verification. Load Groups - total active load groups. Click to display the Active Wireless Load Groups report. Local Stations - total number of active mobile stations. Click to display the All Active Client report. Local & Foreign - total number of active and foreign stations. Click to display the All Active Client report. VNS - total defined VNSs (enabled and disabled). Click to display the total number of enabled and disabled VNS assignments, respectively, configured on the system. Availability - status of the controller availability. Click to display controller settings (Stand-alone, Paired, Fast Failover FFO). Mobility Tunnels - status of the mobility tunnel. Click to display controller settings.
Admin Sessions	<p>Displays information on the total number of recent administrative activities including:</p> <ul style="list-style-type: none"> Read/Write sessions - total number of currently active GUI and CLI (either SSH or serial console ones) Read/Write sessions. Read-only sessions - total number of currently active GUI and CLI (either SSH or serial console ones) Read only sessions. Guest Access sessions - total number of currently active GuestPortal Manager sessions that can only be achieved through the GUI. Auth Type - lists the presently configured login mode. <p>Click each heading to access the Wireless Controller > Login Management screen. For more information, see Configuring the Login Authentication Mode on page 75.</p>
Stations by Protocol	<p>Displays a graphical representation of the total number of active stations grouped by protocol.</p> <p>Click the Stations by Protocol heading to access the All Active Clients Report. For more information, see Viewing Statistics for APs on page 627.</p>
APs by Channel	<p>Displays a graphical representation of the total number of active stations and the number of APs.</p> <p>Click the APs by Channel heading to access the Active Wireless AP Report. For more information, see Viewing Statistics for APs on page 627.</p>
Stations by AP	<p>Displays a graphical representation of the total number of active APs grouped by channel.</p> <p>Click the Status by AP heading to access the Active Clients by Wireless APs Report. For more information, see Viewing Statistics for APs on page 627.</p>

Table 5: Wireless Assistant Home Screen (continued)

Home Screen Heading	Description
Applications by <i>WLAN</i>	<p>If Application Visibility is enabled on the WLAN Configuration screen, a pie chart displaying the top five applications on that WLAN displays. If Application Visibility is not enabled, click Enable Application Visibility to display the Apps, operating systems, and devices used by clients.</p> <p>The Application Visibility option displays the following information for clients associated with a selected WLAN:</p> <ul style="list-style-type: none"> • IPv4 and IPv6 Addresses • Host Name • Operating System • Device Type • Top 5 Application Groups by Throughput (2-minute interval) • Top 5 current Application Groups by Bytes, from session start. • Throughput chart for an application group. • Average TCP Round Trip Time. • Average DNS Round Trip Time. <p>For more information, see Enabling Application Visibility with Device Identification on page 626 and Device Identification on page 625.</p>

Table 5: Wireless Assistant Home Screen (continued)

Home Screen Heading	Description
Licensing	<p>Displays licensing information including:</p> <ul style="list-style-type: none"> License mode: License Manager can operate in Lone or Paired mode. <p>Lone (standalone) - Only local APs are counted against locally installed capacity keys. ALL Radar In-Service and Guardian APs are counted against locally installed Radar keys. This is the default license mode. License Manager switches to Paired mode on the following conditions: Availability is enabled while License Manager is running and it receives a license request or Availability is enabled before the License Manger starts up and the database has counters for the peers capacity and Radar keys.</p> <p>Paired - Both local and foreign APs are counted against sum of locally installed capacity keys and capacity keys, pooled from the peer controller. ALL Radar In-Service and Guardian APs are counted against sum of locally installed Radar keys, installed on the peer controller. License Manager switches to Lone (standalone) mode if Availability is disabled or if the peer IP address is changed.</p> <ul style="list-style-type: none"> Unused AP Licenses: total number of unassigned AP licenses (for more information, see Applying Product License Keys on page 47). Local AP Licenses: total number of AP licenses local to the primary controller. Foreign AP Licenses: total number of AP licenses local to the secondary (backup) controller. Local Radar Licenses: total number of Radar licenses local to the primary controller. Foreign Radar Licenses: total number of Radar licenses local to the secondary (backup) controller. Unused Radar Licenses: total number of unassigned licenses for Radar (for more information, see Radar License Requirements on page 565). Days Remaining: number of days remaining on this license key. Regulatory Domain: Domain information for this license period. <p>Click the Licensing heading to access the Wireless Controller > Software Maintenance screen. For more information, see Installing the License Keys on page 49.</p>
Health	<p>Displays network health statistics including:</p> <ul style="list-style-type: none"> Local AP Uptime (min) APs with > 30 clients APs in low power mode <p>This feature is for AP39xx only. This option displays when there is one or more AP39xx in low power mode. Click to display details of the AP.</p> <ul style="list-style-type: none"> Failed VNS RADIUS TxS <p>Click each heading to access the Active Wireless APs Report. For more information, see Viewing Statistics for APs on page 627.</p>

Table 5: Wireless Assistant Home Screen (continued)

Home Screen Heading	Description
Radar	<p>Displays totals for the following security related statistics:</p> <ul style="list-style-type: none"> • AP Remote Access - click to access the APs > AP Registration page • Unsecured WLANs - click to access the WLAN Security Report • Uncategorized APs - click to access the list of Uncategorized APs • Active Threats - click to access the Active Threats Report • Active Countermeasures - click to access the Active Countermeasures Report • APs denied by license - click to access the list of APs denied by license constraints. <p>For more information, see Wireless AP Registration on page 123, and Working with Radar Reports on page 593.</p>
Events	<p>Displays major events that impact network performance and efficiency. Each event listed includes a timestamp of the event, the type or classification of the event, which component is impacted by the event, and a log message providing specific information for the event.</p> <p>Click the Events heading to access the Log > Logs & Traces page. For more information, see Working with Reports and Statistics on page 621.</p>

Working with the Basic Installation Wizard

The Extreme Networks ExtremeWireless system provides a basic installation wizard that can help administrators configure the minimum controller settings that are necessary to deploy a functioning ExtremeWireless system solution on a network.

Use the Basic Installation Wizard to quickly configure the controller for deployment, and later to revise the controller configuration as needed.

The Basic Installation Wizard launches when you log on to the controller for the first time and when the system has been reset to the factory default settings. You can also launch the wizard from the left pane of the controller **Configuration** screen anytime.

To configure the controller using the Basic Installation Wizard:

- 1 Log on to the controller. For more information, see [Logging on to the ExtremeWireless Appliance](#) on page 33.
- 2 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.

- 3 In the left pane, click **Administration** > **Installation Wizard**.

The **Basic Installation Wizard** screen displays.

- 4 In the **Time Settings** section, configure the controller timezone:
- **Continent or Ocean** — Select the continent for the time zone.
 - **Time Zone Region** — Select the appropriate time zone region for the selected continent.
- 5 To configure the controller's time, do one of the following:
- To manually set the controller time, click **Set time**. The Year, Month, Day, HR, and Min. fields display, where you can use the drop-down lists to specify the time values.
 - To use the controller as the NTP time server, select the **Run local NTP Server** option. In the **Server** field, enter the IP address or Domain Name for the NTP server.
 - To use NTP to set the controller time, select the **Use NTP** option, and then type the IP address of an NTP time server that is accessible on the enterprise network.

The Network Time Protocol is a protocol for synchronizing the clocks of computer systems over packet-switched data networks.

- 6 In the **Server** field, enter the IP address or Domain Name for the NTP server.



Note

The Server Address field supports both IPv4 and IPv6 addresses.

- 7 In the **Topology Configuration** section, the physical interface of the controller data port, the **IP Address** and **Netmask** values for the data port, and the **VLAN ID** display as read-only values.
For information on how to obtain a temporary IP address from the network, click **How to obtain a temporary IP address**.
- 8 Click **Next**. The **Management** screen displays

Basic Installation Wizard - Management Screen

The **Management** screen displays:

Management

AP Password

SSH Access Password:

Confirm Password:

Management Port

Static IP Address: ***Verify your configuration before saving. Improper configuration may result in the controller becoming unreachable via its management port.**

Netmask:

Gateway:

Static IPv6 Address:

Prefix Length:

Gateway:

SNMP

Mode: ▼

Syslog Server

Enable

OSPF

Enable

- 1 In the **AP Password** section, enter a password for the AP. Click **Unmask** to display the password characters as you type. Access Points are shipped with default passwords. You must create a new SSH Access Password here.



Note

Passwords can include the following characters: A-Z a-z 0-9 -!@#%&^*()_+|=\\{}[];<>?., Password cannot include the following characters: / ` ' " : or a space.

- 2 In the **Management Port** section, confirm the port configuration values that were defined when the controller was physically deployed on the network. If applicable, edit these values:
 - **Static IP Address** — Displays the IPv4 address for the controller’s management port. Revise this as appropriate for the enterprise network.
 - **Netmask** — Displays the appropriate subnet mask for the IP address to separate the network portion from the host portion of the address.
 - **Gateway** — Displays the default gateway of the network.
 - **Static IPv6 Address** — Displays the IPv6 address for the controller’s management port. Revise this as appropriate for the enterprise network.
 - **Prefix Length** — Length of the IPv6 prefix. Maximum is 64 bits.
 - **Gateway** — Displays the default gateway of the network.
- 3 In the **SNMP** section, click **V2c** or **V3** in the **Mode** drop-down list to enable *SNMP (Simple Network Management Protocol)*, if applicable.

If you selected V2c, the Community options display:

- **Read Community** — Type the password that is used for read-only SNMP communication.
- **Write Community** — Type the password that is used for write SNMP communication.
- **Trap Destination** — Type the IP address of the server used as the network manager that will receive SNMP messages.



Note

The Trap Destination Address field supports both IPv4 and IPv6 addresses.

If you selected V3, the Syslog Server options display:

- **Enable** — Click to enable Syslog Server.
 - **IP Address** — Enter the IP address for the Syslog Server.
- 4 In the **OSPF** section, select the **Enable** check box to enable *OSPF*, if applicable. Use OSPF to allow the controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation.

Do the following:

- **Area ID** — Type the desired area. Area 0.0.0.0 is the main area in OSPF.
- 5 In the **Syslog Server** section, select the **Enable** check box to enable the syslog protocol for the controller, if applicable. Syslog is a protocol used for the transmission of event notification messages across networks.

In the **IP Address** field, type the IP address of the syslog server.



Note

The Syslog Server IP Address field supports both IPv4 and IPv6 addresses.

- 6 Click **Next**. The **Services** screen displays.

Basic Installation Wizard - Services Screen

Services

RADIUS

Enable Server Alias:

IP Address:

Shared Secret:

Mobility

Enable

Default VNS

Enable **Type:** Bridged At AP **WPA-PSK key:** MobilityMadeEasy

Name: Wireless **SSID:** Wireless

Back **Finish** **Cancel**

- 1 In the **RADIUS** section, select the **Enable** check box to enable RADIUS login authentication, if applicable.

RADIUS login authentication uses a RADIUS server to authenticate user login attempts. RADIUS is a client/server authentication and authorization access protocol used by a network access server (NAS) to authenticate users attempting to connect to a network device.

Do the following:

- **Server Alias** — Type a name that you want to assign to the RADIUS server. You can type a name or IP address of the server.
- **IP Address** — Type the RADIUS server’s hostname or IP address.
- **Shared Secret** — Type the password that will be used to validate the connection between the controller and the RADIUS server.

- 2 In the **Mobility** section, select the **Enable** check box to enable the controller mobility feature, if applicable. Mobility allows a wireless device user to roam seamlessly between different APs on the same or different controllers.

A dialog informs you that NTP is required for the mobility feature and prompts you to confirm you want to enable mobility.

**Note**

If the ExtremeWireless Appliance is configured as a mobility agent, it will act as an NTP client and use the mobility manager as the NTP server. If the appliance is configured as a mobility manager, its local NTP will be enabled for the mobility domain.

- 3 Click **OK** to continue, and then do the following:
 - **Role** — Select the role for the controller, **Manager** or **Agent**. One controller on the network is designated as the mobility manager and all other controllers are designated as mobility agents.
 - **Port** — Click the interface on the controller to be used for communication between mobility manager and mobility agent. Ensure that the selected interface is routable on the network. For more information, see [Configuring Mobility](#) on page 555.
 - **Manager IP** — Type the IP address of the mobility manager port if the controller is configured as the mobility agent.
- 4 In the **Default VNS** section, select the **Enable** check box to enable a default VNS for the controller.

**Note**

Refer to [Virtual Network Services](#) on page 22 for more information about the default VNS.

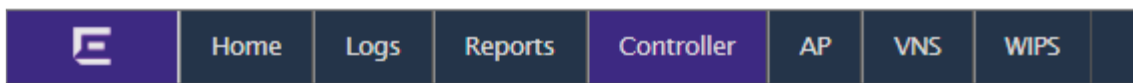
The default VNS parameters display.


- 5 Click **Finish**.

The **Success** screen displays.

Basic Installation Wizard - Success Screen

- 1 We recommend that you change the factory default administrator password.



Success! 

The controller is configured and ready for use. Click Close to exit.

In order to use SNMP V3, you need to create SNMP user accounts using the SNMP page.

It is highly recommended that you change the factory default password.

New Password:

Confirm Password:

- 2 To change the administrator password:
 - a Type a new administrator password in the **New Password**.
 - b Confirm the new password in the **Confirm Password** field.
 - c Click **Save**. Your new password is saved.
- 3 Click **OK**, and then click **Close**.

Note



The ExtremeWireless Appliance reboots after you click Save if the time zone is changed during the Basic Install Wizard. If the IP address of the management port is changed during the configuration with the Basic Install Wizard, the ExtremeWireless Assistant session is terminated and you will need to log back in with the new IP address.

The **Wireless Assistant** home screen displays.

Configuring the ExtremeWireless Appliance for the First Time

After the ExtremeWireless Appliance is deployed, perform the following configuration tasks:

- [Changing the Administrator Password](#) on page 46
- [Applying Product License Keys](#) on page 47
- [Setting Up the Data Ports](#) on page 51
- [Setting Up Internal VLAN ID and Multicast Support](#) on page 58
- [Setting Up Static Routes](#) on page 59
- [Setting Up OSPF Routing](#) on page 61
- [Configuring Filtering at the Interface Level](#) on page 65
- [Protecting Controller Interfaces and the Internal Captive Portal Page](#) on page 69
- [Configuring the Login Authentication Mode](#) on page 75
- [Configuring SNMP](#) on page 85
- [Configuring Network Time](#) on page 89
- [Configuring DNS Servers for Resolving Host Names of NTP and RADIUS Servers](#) on page 94

The basic installation wizard automatically configures aspects of the controller deployment. You can modify that configuration according to your network specifications.

Changing the Administrator Password

Extreme Networks recommends that you change your default administrator password once your system is deployed. The ExtremeWireless Appliance default password is abc123. When the controller is installed and you elect to change the default password, the new password must be a minimum of eight characters.

The minimum eight character password length is not applied to existing passwords. For example, if a six character password is already being used and an upgrade of the software is performed, the software does not require the password to be changed to a minimum of eight characters. However, once the upgrade is completed and a new account is created, or the password of an existing account is changed, the new password length minimum will be enforced.

To Change the Administrator Password:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Login Management**.
- 3 In the Full Administrator table, click the administrator user name.
- 4 In the **Password** field, type the new administrator password.
- 5 In the **Confirm Password** field, type the new administrator password again.
- 6 Click **Change Password**.

Note



The ExtremeWireless Controller provides you with local login authentication mode, the RADIUS-based login authentication mode, and combinations of the two authentication modes. The local login authentication is enabled by default. For more information, see [Configuring the Login Authentication Mode](#) on page 75.

Applying Product License Keys

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

The key strings can be classified into the following variants:

- **Activation Key** — Activates the software. This key is further classified into sub-variants:
 - **Temporary Activation Key** — Activates the software for a trial period of 90 days.
 - **Permanent Activation Key** — Activates the software for an infinite period.
 - **Cloud provider license.**
 - **Subscription license.**



Note

You must obtain a specific activation key to run release v10.01 or later. Once installed, the number of available Radar licenses increments by 2.

- **Option Key** — Activates the optional feature:
 - **Capacity Enhancement Key Format** — For AP:

Enhances the capacity of the controller to manage additional APs.

You may have to add multiple capacity enhancement keys to reach the ExtremeWireless's limit. Depending on the appliance model, a capacity enhancement key adds the following APs:

- C5110 — Adds 25 wireless APs
- C5210 — Adds 25 or 100 wireless APs
- C5215 — Adds 25 or 100 wireless APs
- C4110 — Adds 25 wireless APs
- C25 — Adds 1 or 16 wireless APs
- C35 — Adds 1 or 16 wireless APs
- V2110 — Adds 1 or 16 wireless APs



Note

If you connect additional wireless APs to an ExtremeWireless controller that has a permanent activation key without installing a capacity enhancement key, a grace period of seven days will start. You must install the correct key during the grace period. If you do not install the key, the controller will start generating event logs every 15 minutes, indicating that the key is required. In addition, you will not be able to edit the Virtual Network Services (VNS) parameters.

- **Capacity Enhancement Key Format** — For Radar:

Enhances the capacity of the controller to manage Radar licenses for multiple APs. Radar capacity licenses are only required for In-Service Scan Profiles (for more information, see [Radar License Requirements](#) on page 565). The capacity enhancement key includes a capacity increment which determines the number of APs supported as follows:

License format: RADCAP<nnn> (where <nnn> is the capacity increment):

- RADCAP001 — Adds 1 wireless AP
- RADCAP016 — Adds 16 wireless APs

RADCAPO25 — Adds 25 wireless APs

RADCAP100 — Adds 100 wireless APs



Note

Any AP assigned to an In-Service scan profile counts as 1 against the licensed Radar capacity.

The controller can be in the following licensing modes:

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

A temporary activation key is valid for 90 days. Once the 90 days are up, the temporary key expires. You must get a permanent activation key and install it on the controller. If you do not install a permanent activation key, the controller will start generating event logs every 15 minutes, indicating that an appropriate license is required for the current software version. In addition, you will not be able to edit the Virtual Network Services (VNS) parameters.

- **Cloud Provider** — A Cloud Provider license is valid for a period of 5 years. License pooling is not supported because the values are set at the platform limits. Cloud Provider licenses enable local APs with the system limit of the platform, while the radar licenses are set at twice the system limits. e.g. for V2110 medium, local AP licenses available are 250 and Local radar licenses available are 500.
- **Subscription** — A subscription license can be generated for a period between 1 to 255 days. License pooling is not supported because the values are set at the platform limits. A Subscription license enables local APs with the system limit of the platform, while the radar licenses are set at twice the system limits. e.g. for V2110 medium, local AP licenses available are 250 and Local radar licenses available are 500.
- **Licensed with permanent activation key** — A permanent activation key is valid for an infinite period. In addition, unlike the temporary activation key, the permanent activation key allows you to operate a stipulated number of the APs, depending upon the platform type. If you want to connect additional APs, you have to install a capacity enhancement key. You may even have to install multiple capacity enhancement keys to reach the controller's limit.

The [Table 6](#) lists the platform type and the corresponding number of the APs allowed by the permanent activation key.

Table 6: Platform Type / Wireless APs Allowed by Permanent Activation Key

Platform	Wireless APs permitted by permanent activation key	Platform's optimum limit	Number of capacity enhancement keys to reach the optimum limit
C25	16	50	4 to 34 (depending on the enhancement license type used)
C35	50	125	15 to 75 (depending on the enhancement license type used)

Table 6: Platform Type / Wireless APs Allowed by Permanent Activation Key (continued)

Platform	Wireless APs permitted by permanent activation key	Platform's optimum limit	Number of capacity enhancement keys to reach the optimum limit
C4110	50	250	8
C5110	150	525	15
C5210	100	1000	9 to 36 (depending on the enhancement license type used)
C5215	100	1000	9 to 36 (depending on the enhancement license type used)
V2110 (Small)	8	50	17 to 42 (depending on the enhancement license type used)
V2110 (Medium)	8	250	12 to 242 (depending on the enhancement license type used)
V2110 (Large)	8	525	37 to 517 (depending on the enhancement license type used)

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

The controller can be in an unlicensed state for an infinite period. However, if you install a temporary activation key, the unlicensed state is terminated. After the validity of a temporary activation key and the related grace period expire, the controller generates event logs every 15 minutes, indicating that an appropriate license is required for the current software version. In addition, you will not be able to edit the Virtual Network Services (VNS) parameters.

License Pooling

If the controller is paired with an availability partner, you can redistribute licenses when a Capacity Enhancement Key (AP or Radar) is installed. Both controllers must be running at least v9.01 and both members must have a permanent license key. Separate pools will be introduced for each type of license, and licenses installed on either member of an availability pair are shared across the pair automatically. License pooling is supported in fast failover and legacy availability setups. The limit of distribution is set by the license key; therefore if a controller has two keys of 25 APs each, then you will be allowed to transfer 25 or 50 APs to the former peer controller (for more information, see [Availability](#) on page 537).

License pooling is not supported for Cloud Provider and Subscription license types since the values are already set at the platform system limits.

Installing the License Keys

This section describes how to install the license key on the controller. It does not explain how to generate the license key. For information on how to generate the license key, see the ExtremeWireless License Certificate, which is sent to you via traditional mail.

For more information on licensing, see [Licensing Considerations](#) on page 108.

You have to type the license keys on the Wireless Assistant GUI.

To install the license keys:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Administration > Software Maintenance**.
- 3 Click the **EWC Product Keys** tab.

The bottom pane displays the license summary.

The screenshot shows the 'EWC Product Keys' tab in the GUI. It includes a top navigation bar with 'Controller' selected. Below it are tabs for 'EWC Software', 'Backup', 'Restore', and 'EWC Product Keys'. The 'EWC Product Keys' tab is active, displaying two input fields: 'Subscription / Activation License Key' and 'Option Key'. Each field has an 'Apply' button next to it. Below the input fields, the license key format is shown as 'AAAAAAA-11111111-11111111-11111111-11111111'. Under the 'Option Key' field, the capacity enhancement key format is shown, with examples for APs and Radar. A red warning message '*Option Key limit reached,' is displayed. At the bottom, a 'License Summary' section provides details: Locking ID: 00-50-56-01-AB-46, Regulatory Domain: European Union (& Rest of World), Number of Licensed APs: 50, Number of Licensed APs for Radar: 100, Subscription License: 103 day(s) left in this 120-day license period, and License expires on: Feb 10, 2018. A 'View Installed Keys' button is located at the bottom right of the summary section.

Figure 8: Product Keys Tab

- 4 If you are installing a temporary or permanent activation license key, type the key in the **Activation Key** field, and then click the **Apply Activation Key** button.
- 5 If you are installing a capacity enhancement, type the key in the **Option Key** field, and then click the **Apply Option Key** button.

- 6 To view installed keys, click **View Installed Keys**. The **Installed Licensed Keys** dialog displays.

Installed Licensed Keys

Activation key: PRDKVFCC-N8A7X8ZH-NZGO4GAQ-4CFKN5Z3-75POQ226

Licensed Software Release: 10.01.01.0109

Regulatory Domain: FCC

Option Keys:

Feature	License Key	Description

Licensed AP Totals:

Base Number of APs:	8
Option Number of APs:	0
<hr/>	
Total Licensed APs:	8

APs Licensed for Radar:

Base Number of APs licensed for Radar:	2
Option Number of APs licensed for Radar:	0
<hr/>	
Total Licensed APs for Radar:	2

Figure 9: Installed License Keys

Setting Up the Data Ports

A new controller is shipped from the factory with all its data ports set up. Support of management traffic is disabled on all data ports. By default, data interface states are enabled. A disabled interface does not allow data to flow (receive/transmit).

Physical ports are represented by the L2 (Ethernet) Ports. The L2 port can be accessed from **L2 Ports** tabs under ExtremeWireless Controller Configuration. The L2 Ports cannot be removed from the system but their operational status can be changed. Refer to [Viewing and Changing the L2 Ports Information](#) on page 52.

Link Aggregation ports are represented by the L2 (peer-to-peer) *LAG (Link Aggregation Group)* Ports. The L2 port and Topology information can be accessed from **L2 Ports** and **Topology** tabs under ExtremeWireless Controller Configuration. The LAG L2 Ports cannot be removed from the system but their operational status can be changed. Refer to [Viewing and Changing the L2 Ports Information](#) on page 52.



Note

You can redefine a data port to function as a Third-Party AP Port. Refer to [Viewing and Changing the Physical Topologies](#) on page 54 for more information.

Viewing and Changing the L2 Ports Information

To view and change the L2 port information:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network** > **L2 Ports**. The **L2 Ports** tab is displayed.

L2 Ports					
Physical L2 Ports					
Enable	Port	MAC	Untagged Vlan	Tagged Vlan	
<input checked="" type="checkbox"/>	esa0	00:0C:29:71:D8:84	3546		
<input checked="" type="checkbox"/>	esa1	00:0C:29:71:D8:8E		445, 446, 775	
<input checked="" type="checkbox"/>	Admin	00:50:56:01:AB:46	U		

- 3 The **L2 Ports** tab presents the Physical (that is, Ethernet) and **LAG** (peer to peer) data ports that exist on the controller. These ports cannot be deleted and new ones cannot be created.

LAG ports are statically configured by adding/removing physical ports from the LAG. Physical port belong to at most one LAG at one time. L2 port attached to a LAG port does not have any properties and could not be attached to any topology. The L2 ports attached to LAG ports can be enabled or disabled. Optional, if changes occur to the port physical parameters (speed, half or full duplex), a warning will be displayed to indicate that the L2 port does not meet LAG conditions.

Considerations for attaching/detaching regular L2 ports to LAG ports:

- Regular L2 port should not have any bridged and physical topologies associated with the port.
- Regular L2 port should not be disabled.
- L2 ports can be detached from LAG ports regardless of any topologies attached to the LAG port.
- If the L2 port is the last remaining in LAG, a warning will be issued. If last port of the LAG has been detached, the LAG should be in operational DOWN state.
- After detaching the L2 port, it could be attached to any bridged or physical topology or points via a routing table to the port any Routed topology.
- Jumbo Frames support is a feature that allows the configuration of physical Maximum Transmission Unit (MTU) sizes larger than the standard 1500 bytes on the AP and controller. When Jumbo Frames is enabled, the maximum MTU is 1800 bytes.

- 4 Assigning any bridged or physical topology without specifying an L2 port is not supported. However, you can move any bridged and physical topology to either a physical or LAG L2 port.

Physical:

- C5110 — Three data ports, displayed as esa0, esa1, and esa2.
- C5210 — Four data ports, displayed as esa0, esa1, esa2, and esa3.
- C5215 — Four data ports, displayed as esa0, esa1, esa2, and esa3.
- C4110 — Four data ports, displayed as Port1, Port2, Port3, and Port4.
- C25 — Two data ports, displayed as esa0 and esa1.
- C35 — Four data ports, displayed as esa0, esa1, esa2, and esa3.
- V2110 — Two data ports, displayed as esa0 and esa1.

Link Aggregation:

- C5110 — One data port, displayed as lag1
 - C5210 — Two data ports, displayed as lag1 and lag2.
 - C5215 — Two data ports, displayed as lag1 and lag2.
 - C4110 — Two data ports, displayed as lag1 and lag2.
 - C35 — Two data ports, displayed as lag1 and lag2.
 - C25 — One data port, displayed as lag1.
- 5 An “Admin” port is created by default. This represents a physical port, separate from the other data ports, being used for management connectivity. For more information, see [Configuring the Admin Port](#) on page 263.

Parameters displayed for the L2 Ports are:

- Operational status, represented graphically with a green checkmark (UP) or red X (DOWN). This is the only configurable parameter.
- Port name, as described above.
- MAC address, as per Ethernet standard.
- Untagged VLAN, displays the associated untagged VLAN ID. This ID is unique among topologies.
- Tagged VLAN, displays the associated tagged VLAN ID.
- Attached Physical L2 Ports (Link Aggregation L2 Ports only) select the physical L2 ports associated with the link aggregation L2 Ports.



Note

Refer to [Viewing and Changing the Physical Topologies](#) on page 54 for more information about L2 port topologies.

- 6 If desired, change the operational status by clicking the Enable check box.
- You can change the operational state for each port. By default, data interface states are enabled. If they are not enabled, you can enable them individually. A disabled interface does not allow data to flow (receive/transmit).
- 7 If support of MTU sizes above 1500 bytes is required, click **Enable Jumbo Frames support**. This will extend the MTU size to 1800 bytes on the data link layer.
- Enabling Jumbo Frames support requires that port speed to be 1Gbps or higher on the controller and the APs which support Jumbo Frames. Jumbo Frames are not supported on 10 or 100 Mbps speeds.

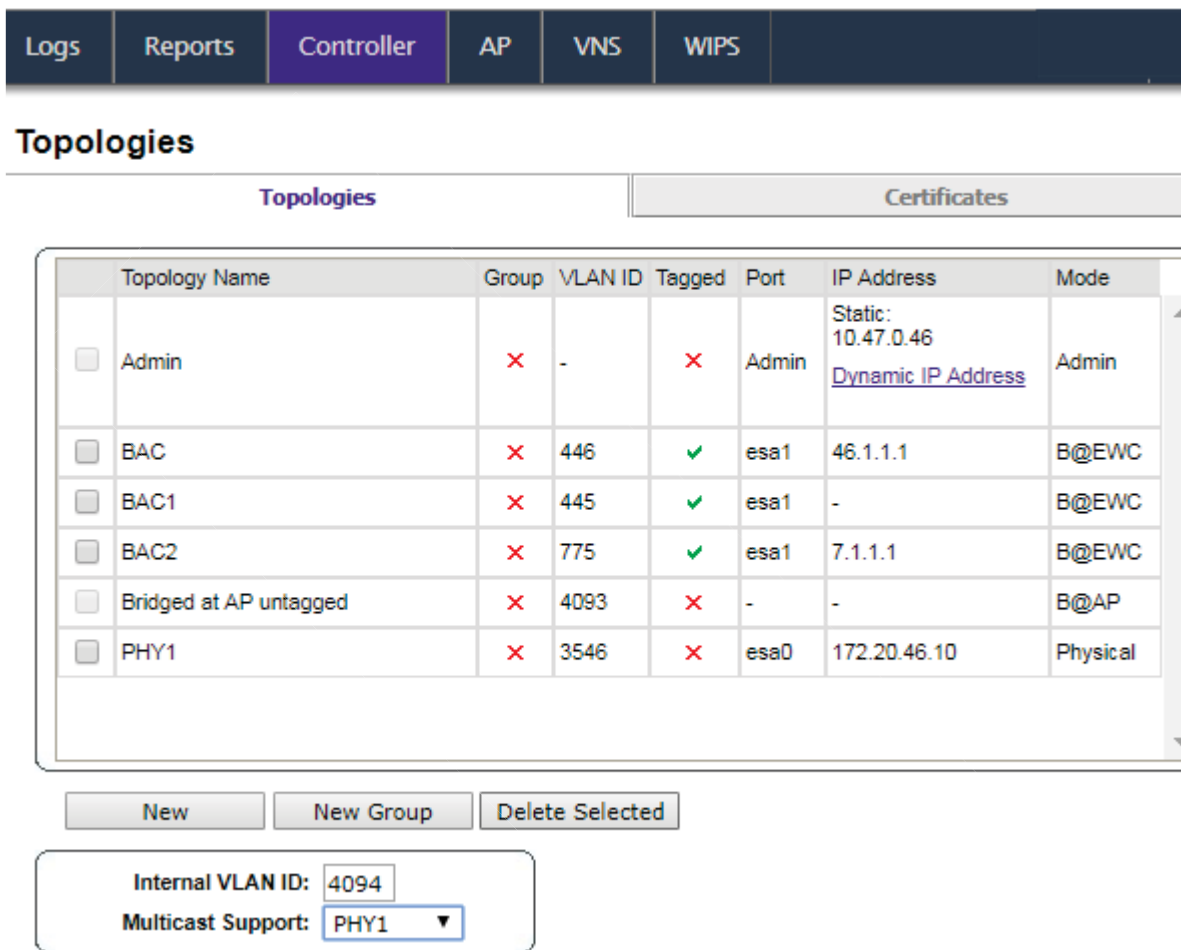
Viewing and Changing the Physical Topologies

To view and change the L2 Port topologies:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network > Topologies**.

An associated topology entry is created by default for each L2 Port with the same name.

The **Topologies** tab is displayed.



The screenshot displays the 'Topologies' configuration page. At the top, there is a navigation bar with tabs for 'Logs', 'Reports', 'Controller' (selected), 'AP', 'VNS', and 'WIPS'. Below this, the 'Topologies' section is active, showing a table of topology entries. The table has columns for 'Topology Name', 'Group', 'VLAN ID', 'Tagged', 'Port', 'IP Address', and 'Mode'. Below the table are three buttons: 'New', 'New Group', and 'Delete Selected'. At the bottom, there are two input fields: 'Internal VLAN ID' with the value '4094' and 'Multicast Support' with a dropdown menu showing 'PHY1'.

Topology Name	Group	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	×	-	×	Admin	Static: 10.47.0.46 Dynamic IP Address	Admin
<input type="checkbox"/> BAC	×	446	✓	esa1	46.1.1.1	B@EWC
<input type="checkbox"/> BAC1	×	445	✓	esa1	-	B@EWC
<input type="checkbox"/> BAC2	×	775	✓	esa1	7.1.1.1	B@EWC
<input type="checkbox"/> Bridged at AP untagged	×	4093	×	-	-	B@AP
<input type="checkbox"/> PHY1	×	3546	×	esa0	172.20.46.10	Physical

Buttons:

Internal VLAN ID:
 Multicast Support:

- To make changes, select a specific topology.
The **Edit Topology** dialog appears.

For the data ports predefined in the system, Name and Mode are not configurable.

- Optionally, configure one of the physical topologies for Third Party AP connectivity by clicking the **3rd Party AP Topology** check box.

You must configure a topology to which you will be connecting third-party APs by checking this box. Only one topology can be configured for third-party APs.

Third-party APs must be deployed within a segregated network for which the controller becomes the single point of access (i.e., routing gateway). When you define a third-party AP topology, the interface segregates the third-party AP from the remaining network.

- To configure an interface for VLAN assignment, configure the VLAN Settings in the **Layer 2** box.
When you configure a controller port to be a member of a VLAN, you must ensure that the VLAN configuration (VLAN ID, tagged or untagged attribute, and Port ID) is matched with the correct configuration on the network switch.
- To replicate topology settings, click **Synchronize** in the **Status** field.
- If the desired IP configuration is different from the one displayed, change the **Interface IP** and **Mask** accordingly in the **Layer 3** box.

For this type of data interface, the Layer 3 check box is selected automatically. This allows for IP Interface and subnet configuration together with other networking services.

- 8 The **MTU** value specifies the Maximum Transmission Unit or maximum packet size for this topology. The fixed value is 1500 bytes for physical topologies.

If you are using *OSPF*, be sure that the MTU of all the interfaces in the OSPF link match.

Note



If the routed connection to an AP traverses a link that imposes a lower MTU than the default 1500 bytes, the controller and AP participate in automatic MTU discovery and adjust their settings accordingly. At the controller, MTU adjustments are tracked on a per AP basis. If the ExtremeWireless software cannot discover the MTU size, it enforces the static MTU size.

- 9 To enable AP registration through this interface, select the **AP Registration** check box. Wireless APs use this port for discovery and registration. Other controllers can use this port to enable inter-controller device mobility if this port is configured to use SLP or the controller is running as a manager and SLP is the discovery protocol used by the agents.
- 10 To enable management traffic, select the **Management Traffic** check box. Enabling management provides access to *SNMP* (v1/v2c, v3), SSH, and HTTPs management interfaces.

Note



This option does not override the built-in protection filters on the port. The built-in protection filters for the port, which are restrictive in the types of packets that are allowed to reach the management plane, are extended with a set of definitions that allow for access to system management services through that interface (SSH, SNMP, HTTPS:5825).

- 11 To enable the local *DHCP* Server on the controller, in the **DHCP** field, select **Local Server**. Then, click on the **Configure** button to open the **DHCP configuration** pop-up window.

Note



The local DHCP Server is useful as a general-purpose DHCP Server for small subnets.

- a In the **Domain Name** field, type the name of the domain that you want the APs to use for DNS Server's discovery.
- b In the **Lease (seconds) default** field, type the time period for which the IP address will be allocated to the APs (or any other device requesting it).
- c In the **Lease (seconds) max** field, type the maximum time period in seconds for which the IP address will be allocated to the APs.
- d In the **DNS Servers** field, type the DNS Server's IP address if you have a DNS Server.
- e In the **WINS** field, type the WINS Server's IP address if you have a WINS Server.

Note

You can type multiple entries in the **DNS Servers** and **WINS** fields. Each entry must be separate by a comma. These two fields are not mandatory to enable the local DHCP feature.

-
- f In the **Gateway** field, type the IP address of the default gateway.

Note

Since the controller is not allowed to be the gateway for the segment, including APs, you cannot use the Interface IP address as the gateway address for physical and Bridged at Controller topology. For Routed topology, the controller IP address must be the gateway.

-
- g Configure the address range from which the local DHCP Server will allocate IP addresses to the APs.
 - In the **Address Range: from** field, type the starting IP address of the IP address range.
 - In the **Address Range: to** field, type the ending IP address of the IP address range.
 - h Click the **Exclusion(s)** button to exclude IP addresses from allocation by the DHCP Server. The DHCP Address Exclusion window opens.

The controller automatically adds the IP addresses of the Interfaces (Ports), and the default gateway to the exclusion list. You cannot remove these IP addresses from the exclusion list.

Extreme
Connect Beyond the Network

Address Exclusion

Configured DHCP Address Range: **46.1.1.2 - 46.1.1.254**

IP Address(es) to exclude from DHCP Address Range:

Range: From: to:

Single Address:

Comment:

- Select **Range**. In the **From** field, type the starting IP address of the IP address range that you want to exclude from the DHCP allocation.
- In the **To** field, type the ending IP address of the IP address range that you want to exclude from the DHCP allocation.
- To exclude a single address, select the Single Address radio button and type the IP address in the adjacent field.
- In the **Comment** field, type any relevant comment. For example, you can type the reason for which a certain IP address is excluded from the DHCP allocation.
- Click **Add**. The excluded IP addresses are displayed in the **IP Address(es) to exclude from DHCP Address Range** field.
- To delete a IP Address from the exclusion list, select it in the **IP Address(es) to exclude from DHCP Range** field, and then click **Delete**.
- To save your changes, click **OK**.



Note

The Broadcast (B'cast) Address field is view only. This field is computed from the mask and the IP addresses.

Setting Up Internal VLAN ID and Multicast Support

You can configure the Internal VLAN ID, and enable multicast support. The internal VLAN used only internally and is not visible on the external traffic. The physical topology used for multicast is represented by a physical topology to/from which the multicast traffic is forwarded in conjunction with

the virtual routed topologies (and VNSs) configured on the controller. Please note that no multicast routing is available at this time.

To configure the Internal VLAN ID and enable multicast support:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network > Topologies**.

The **Topologies** tab is displayed.

The screenshot shows the 'Topologies' configuration page. At the top, there is a navigation bar with tabs: Logs, Reports, Controller (selected), AP, VNS, and WIPS. Below the navigation bar, the 'Topologies' section is active, showing a table of configurations. The table has columns for Topology Name, Group, VLAN ID, Tagged, Port, IP Address, and Mode. Below the table are buttons for 'New', 'New Group', and 'Delete Selected'. At the bottom, there are input fields for 'Internal VLAN ID' (set to 4094) and 'Multicast Support' (set to PHY1).

Topology Name	Group	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	×	-	×	Admin	Static: 10.47.0.46 Dynamic IP Address	Admin
<input type="checkbox"/> BAC	×	446	✓	esa1	46.1.1.1	B@EWC
<input type="checkbox"/> BAC1	×	445	✓	esa1	-	B@EWC
<input type="checkbox"/> BAC2	×	775	✓	esa1	7.1.1.1	B@EWC
<input type="checkbox"/> Bridged at AP untagged	×	4093	×	-	-	B@AP
<input type="checkbox"/> PHY1	×	3546	×	esa0	172.20.46.10	Physical

Buttons: **New**, **New Group**, **Delete Selected**

Internal VLAN ID:
 Multicast Support:

- 3 In the **Internal VLAN ID** field, type the internal VLAN ID.
- 4 From the **Multicast Support** drop-down list, select the desired physical topology.
- 5 To save your changes, click **Save**.

Setting Up Static Routes

When setting up a controller routing protocol, you must define a default route to your enterprise network, either with a static route or by using the *OSPF* protocol. A default route enables the controller to forward packets to destinations that do not match a more specific route definition.

To Set a Static Route on the controller:

- 1 From the top menu, click **Controller**.
The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Network > Routing Protocols**.
The **Static Routes** tab is displayed.

R#	Dest.Addr	Subnet Mask	Gateway	Interface	O/D
<input type="checkbox"/>	172.20.42.0	255.255.255.0	172.20.46.1	PHY1	on

- 3 To add a new route, click **New**, and in the **Edit route** dialog, enter the following information:
 - In the **Destination Address** field, type the IP address of the destination controller.
To define a default static route for any unknown address not in the routing table, type 0 . 0 . 0 . 0 .
 - In the **Subnet Mask** field, type the appropriate subnet mask to separate the network portion from the host portion of the IP address (typically 255.255.255.0). To define the default static route for any unknown address, type 0 . 0 . 0 . 0 .
 - In the **Gateway** field, type the IP address of the adjacent router port or gateway on the same subnet as the controller to which to forward these packets. This is the IP address of the next hop between the controller and the packet's ultimate destination.
 - Select the **Override dynamic routes** check box to give priority over the OSPF learned routes, including the default route, which the controller uses for routing. This option is enabled by default.
 - To remove this priority for static routes, so that routing is controlled dynamically at all times, clear the **Override dynamic routes** check box.

Note



If you enable dynamic routing (OSPF), the dynamic routes will normally have priority for outgoing routing. For internal routing on the controller, the static routes normally have priority.

- To save your changes, click **Save**.

Viewing the Forwarding Table

You can view the defined routes, whether static or *OSPF*, and their current status in the forwarding table.

To view the forwarding table on the controller:

- From the **Routing Protocols Static Routes** tab, click **View Forwarding Table**. The Forwarding Table is displayed.
- Alternatively, from the top menu, click **Reports**. The **Available AP Reports** screen displays.
- In the left pane, click **Routing Protocols**, then click **Forwarding Table**.

The **Forwarding Table** is displayed.

lab-422-g - Reports - Forwarding Table No refresh Refresh every 30 secs

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.219.40.2	Port1	OSPF	Active
2	0.0.0.0	0.0.0.0	10.219.40.2	Port1	Static	Inactive
3	10.1.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
4	10.2.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
5	10.3.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
6	10.4.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
7	10.5.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
8	10.6.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
9	10.7.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
10	10.8.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
11	10.9.0.0	255.255.0.0	10.219.40.2	Port1	OSPF	Active
12	10.10.10.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
13	10.11.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
14	10.12.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
15	10.13.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
16	10.14.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
17	10.15.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
18	10.16.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
19	10.17.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
20	10.18.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active
21	10.19.0.0	255.255.255.0	10.219.40.2	Port1	OSPF	Active

Data as of Feb 26, 2014 10:56:12 am

This report displays all defined routes, whether static or OSPF, and their current status.

- To update the display, click **Refresh**.

Setting Up OSPF Routing

Open Shortest Path First (OSPF) is a robust link-state routing protocol. OSPF forms adjacencies with neighbors and shares information via the Designated Router (DR) and Backup DR using link state advertisements. Areas in OSPF are used to limit LSAs and summarize routes. Everyone connects to area zero, the backbone.

Related Links

[Enabling OSPF Routing](#) on page 62

[Setting OSPF Routing Settings](#) on page 62

[Confirming OSPF Ports](#) on page 65

Enabling OSPF Routing

To enable *OSPF* (OSPF RFC2328) routing, you must:

- 1 Specify at least one topology on which OSPF is enabled on the Port Settings option of the OSPF tab. This is the interface on which you can establish OSPF adjacency.
- 2 Enable OSPF globally on the controller.
- 3 Define the global OSPF parameters.
- 4 Ensure that the OSPF parameters defined here for the controller are consistent with the adjacent routers in the OSPF area. This consistency includes the following:
 - If the peer router has different timer settings, the protocol timer settings in the controller must be changed to match to achieve OSPF adjacency.
 - The MTU of the ports on either end of an OSPF link must match. The MTU for ports on the controller is fixed at 1500. This matches the default MTU in standard routers. The maximum MTU can be increased to 1800 bytes by enabling Jumbo Frames support (for more information, see [Setting Up the Data Ports](#) on page 51).

It is important to ensure that the MTU of the ports on either end of an OSPF link match. If there is a mismatch in the MTU, then the OSPF adjacency between the controller and the neighboring router might not get established.

Related Links

[Setting Up OSPF Routing](#) on page 61

[Setting OSPF Routing Settings](#) on page 62

[Confirming OSPF Ports](#) on page 65

Setting OSPF Routing Settings

To set OSPF routing global settings on the controller:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network > Routing Protocols**. The **Static Routes** tab is displayed by default.

- 3 Click the **OSPF** tab.

» **View Forwarding Table** **Static Routes** **OSPF**

Global Settings

OSPF Status: **Area id:**

Router id: **Area Type:**

Interface Settings

Topology	Enabled	Authentication	Password	Cost	H / I	D / I	RT / I	Delay

- 4 From the **OSPF Status** drop-down list, click **On** to enable OSPF.
In the **Router ID** field, type the IP address of the controller. This ID must be unique across the OSPF area. If left blank, the OSPF daemon automatically picks a router ID from one of the controller's interface IP addresses.
- 5 In the **Area ID** field, type the area. 0.0.0.0 is the main area in OSPF.
- 6 In the **Area Type** drop-down list, click one of the following:
 - **Default** — The default acts as the backbone area (also known as area zero). It forms the core of an OSPF network. All other areas are connected to it, and inter-area routing happens via a router connected to the backbone area.
 - **Stub** — The stub area does not receive external routes. External routes are defined as routes which were distributed in OSPF via another routing protocol. Therefore, stub areas typically rely on a default route to send traffic routes outside the present domain.
 - **Not-so-stubby** — The not-so-stubby area is a type of stub area that can import autonomous system (AS) external routes and send them to the default/backbone area, but cannot receive AS external routes from the backbone or other areas.
- 7 To save your changes, click **Save**.

- 8 To add a new OSPF interface, click **New** or select a port to configure by clicking on the desired port in the Port Settings table.

The **Edit Port** dialog displays.

- 9 In the **Link Cost** field, type the OSPF standard value for your network for this port. This is the cost of sending a data packet on the interface. The lower the cost, the more likely the interface is to be used to forward data traffic.

Note



If more than one port is enabled for OSPF, it is important to prevent the controller from serving as a router for other network traffic (other than the traffic from wireless device users on routed topologies controlled by the controller). For more information, see [Policy Rules](#) on page 288.

- 10 In the **Authentication** drop-down list, click the authentication type for OSPF on your network: **None** or **Password**. The default setting is **None**.
- 11 If **Password** is selected as the authentication type, in the **Password** field, type the password. If **None** is selected as the Authentication type, leave this field empty. This password must match on either end of the OSPF connection.
- 12 Type the following:
- **Hello-Interval** — Specifies the time in seconds (displays OSPF default). The default setting is 10 seconds.
 - **Dead-Interval** — Specifies the time in seconds (displays OSPF default). The default setting is 40 seconds.
 - **Retransmit-Interval** — Specifies the time in seconds (displays OSPF default). The default setting is 5 seconds.
 - **Transmit Delay**— Specifies the time in seconds (displays OSPF default). The default setting is 1 second.
- 13 To save your changes, click **Save**.

Related Links

[Setting Up OSPF Routing](#) on page 61

[Enabling OSPF Routing](#) on page 62

[Confirming OSPF Ports](#) on page 65

Confirming OSPF Ports

To confirm that the ports are set up for OSPF, and that advertised routes from the upstream router are recognized:

- 1 Click **View Forwarding Table**. The **Forwarding Table** is displayed.
The following additional reports display OSPF information when the protocol is in operation:
 - **OSPF Neighbor** — Displays the current neighbors for OSPF (routers that have interfaces to a common network)
 - **OSPF Linkstate** — Displays the Link State Advertisements (LSAs) received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies.
- 2 To update the display, click **Refresh**.

Related Links

[Setting Up OSPF Routing](#) on page 61

[Enabling OSPF Routing](#) on page 62

[Setting OSPF Routing Settings](#) on page 62

Configuring Filtering at the Interface Level

The ExtremeWireless solution has a number of built-in filters that protect the system from unauthorized traffic. These filters are specific only to the controller. These filters are applied at the network interface level and are automatically invoked. By default, these filters provide stringent-level rules to allow only access to the system's externally visible services. In addition to these built-in filters, the administrator can define specific exception filters at the interface-level to customize network access. These filters depend on Topology Modes and the configuration of an L3 interface for the topology.

For Bridged at Controller topologies, exception filters are defined only if L3 (IP) interfaces are specified. For Physical, Routed, and 3rd Party AP topologies, exception filtering is always configured since they all have an L3 interface presence.

Built-in Interface-based Exception Filters

On the controller, various interface-based exception filters are built in and invoked automatically. These filters protect the controller from unauthorized access to system management functions and services via the interfaces. Access to system management functions is granted if the administrator selects the **allow management traffic** option in a specific topology.

Allow management traffic is possible on the topologies that have L3 IP interface definitions. For example, if management traffic is allowed on a physical topology (esa0), only users connected through ESA0 will be able to get access to the system. Users connecting on any other topology, such as Routed or Bridged Locally at Controller, will no longer be able to target ESA0 to gain management access to the system. To allow access for users connected on such a topology, the given topology configuration itself must have **allow management traffic** enabled and users will only be able to target the topology interface specifically.

On the controller's L3 interfaces (associated with either physical, Routed, or Bridged Locally at Controller topologies), the built-in exception filter prohibits invoking SSH, HTTPS, or SNMP. However, such traffic is allowed, by default, on the management port.

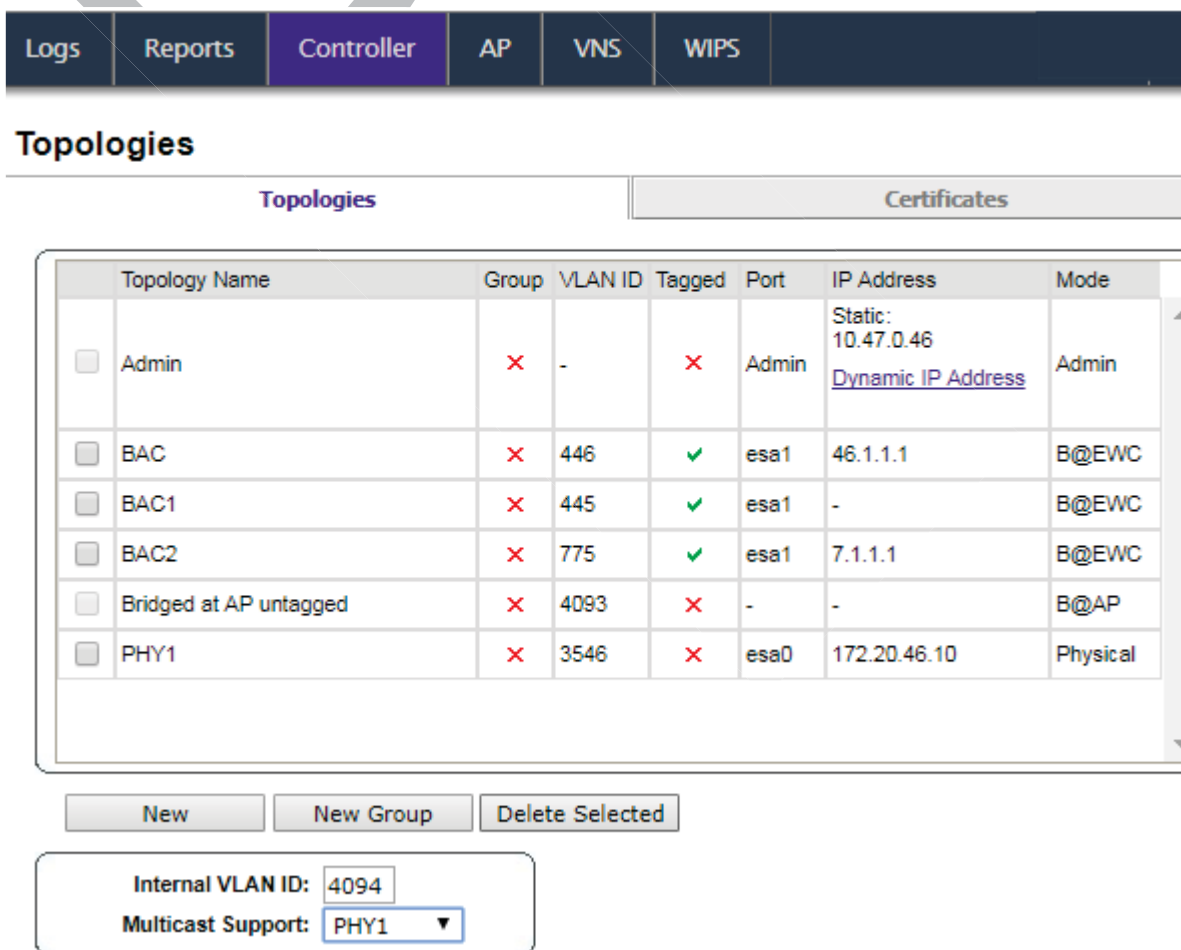
If management traffic is explicitly enabled for any interface, access is implicitly extended to that interface through any of the other interfaces (VNS). Only traffic specifically allowed by the interface's exception filter is allowed to reach the controller itself. All other traffic is dropped. Exception filters are dynamically configured and regenerated whenever the system's interface topology changes (for example, a change of IP address for any interface).

Enabling management traffic on an interface adds additional rules to the exception filter, which opens up the well-known IP(TCP/UDP) ports, corresponding to the HTTPS, SSH, and SNMP applications.

The interface-based built-in exception policy rules, in the case of traffic from wireless users, are applicable to traffic targeted directly for the topology L3 interface. For example, a filter specified by a Role may be generic enough to allow traffic access to the controller's management (for example, Allow All [*. *.*.*]). Exception policy rules are evaluated after the user's assigned filter role, as such, it is possible that the role allows the access to management functions that the exception filter denies. These packets are dropped.

To enable SSH, HTTPS, or SNMP access through a physical data interface:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network > Topologies**. The **Topologies** tab is displayed.



Topology Name	Group	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	×	-	×	Admin	Static: 10.47.0.46 Dynamic IP Address	Admin
<input type="checkbox"/> BAC	×	446	✓	esa1	46.1.1.1	B@EWC
<input type="checkbox"/> BAC1	×	445	✓	esa1	-	B@EWC
<input type="checkbox"/> BAC2	×	775	✓	esa1	7.1.1.1	B@EWC
<input type="checkbox"/> Bridged at AP untagged	×	4093	×	-	-	B@AP
<input type="checkbox"/> PHY1	×	3546	×	esa0	172.20.46.10	Physical

Internal VLAN ID:
 Multicast Support:

- 3 On the **Topologies** tab, click the appropriate data port topology. The **Edit Topology** window displays.

- 4 Select the **Management Traffic** check box if the topology has specified an L3 IP interface presence.
- 5 To save your changes, click **Save**.

Working with Administrator-defined Interface-based Exception Filters

You can add specific policy rules at the interface level in addition to the built-in rules. Such rules give you the capability of restricting access to a port, for specific reasons, such as a Denial of Service (DoS) attack.

The policy rules are set up in the same manner as policy rules defined for a Role — specify an IP address, select a protocol if applicable, and then either allow or deny traffic to that address. For more information, see [Policy Rules](#) on page 288.

The rules defined for port exception filters are prepended to the normal set of restrictive exception filters and have precedence over the system's normal protection enforcement (that is, they are evaluated first).



Warning

If defined improperly, user exception rules may seriously compromise the system's normal security enforcement rules. They may also disrupt the system's normal operation and even prevent system functionality altogether. It is advised to only augment the exception-filtering mechanism if absolutely necessary.

To define interface exception filters:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network > Topologies**. The **Topologies** screen displays.
- 3 Select a topology to be configured. The **Edit Topology** window is displayed.

- If the topology has an L3 interface defined, an **Exception Filters** tab is available. Select this tab. The Exception Filter rules are displayed.

Topology: BAC

General		Multicast Filters		Exception Filters	
Rule	In	Allow	IP : Port	Protocol	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32:22 (SSH)	TCP	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32:20506	TCP	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32:161	TCP	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32:161 (SNMP)	UDP	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32:5825	TCP	
I	dest ▼	<input type="checkbox"/>	46.1.1.1/32:60606	TCP	
I	dest ▼	<input type="checkbox"/>	0.0.0.0/0:50200	TCP	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32:32768-65535	TCP	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32:32768-65535	UDP	
I	dest ▼	<input checked="" type="checkbox"/>	46.1.1.1/32	ICMP	

I: internal (read-only), U: user defined, D: default. Rules with Allow unchecked are denied

Up	Down
Add	Delete
Add Predefined	

Select filter

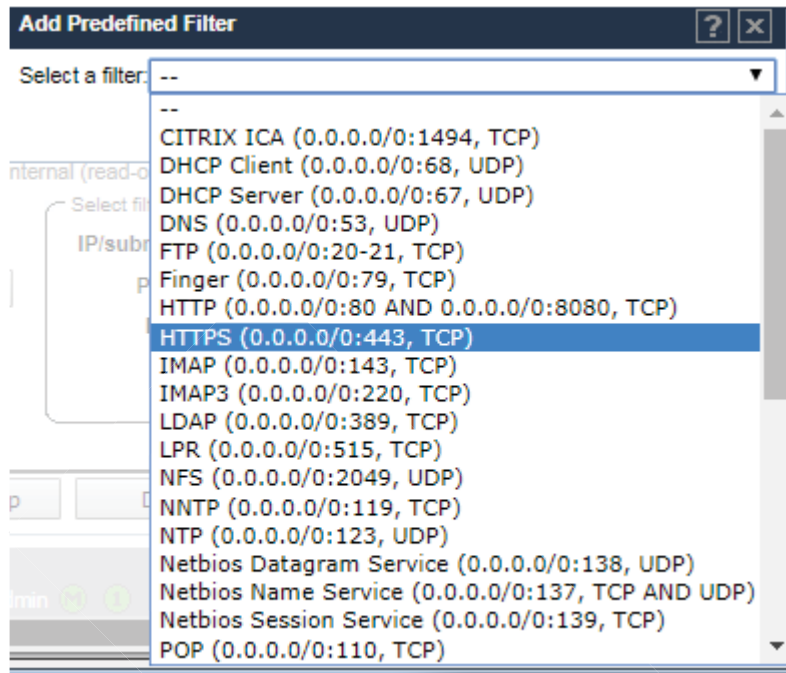
IP/subnet:port:

Protocol:

In Filter:

5 Add rules by either:

- Click **Add Predefined**, select a filter from the drop down list, and click **Add**.



- Click **Add**, configure the following parameters, then click **OK**:

In the **IP / subnet:port** field, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.

In the **Protocol** drop-down list, click the protocol you want to specify for the filter. This list may include UDP, TCP, GRE, IPsec-ESP, IPsec-AH, *ICMP (Internet Control Message Protocol)*. The default is N/A.

- 6 The new filter is displayed in the upper section of the screen.
- 7 Click the new filter entry.
- 8 To allow traffic, select the **Allow** check box.
- 9 To adjust the order of the policy rules, click **Up** or **Down** to position the rule. The policy rules are executed in the order defined here.
- 10 To save your changes, click **Save**.

Protecting Controller Interfaces and the Internal Captive Portal Page

By default, the controller is shipped with a self-signed certificate used to perform the following tasks:

- Protect all interfaces that provide administrative access to the controller
- Protect the internal Captive Portal page

This certificate is associated with topologies that have a configured L3 (IP) interface.

If you continue to use the default certificate to secure the controller and internal Captive Portal page, your web browser will likely produce security warnings regarding the security risks of trusting self-

signed certificates. To avoid the certificate-related web browser security warnings, you can install customized certificates on the controller.



Note

To avoid the certificate-related web browser security warnings when accessing the controller, you must also import the customized certificates into your web browser application.

Before Installing a Certificate

Before you create and install a certificate:

- 1 Select a certificate format to install. The controller supports several types of certificates, as shown in [Table 7](#).

Table 7: Supported Certificate and CA Formats

Certificate Format	Description
PKCS#12	The PKCS#12 certificate (.pfx) file contains both a certificate and the corresponding private key. The controller will accept the PKCS#12 file as long as the format of the private key and certificate are valid.
PEM/DER	The PEM/DER certificate (.crt) file requires a separate PEM/DER private key (.key) file. The controller uses OpenSSL PKCS12 command to convert the .crt and .key files into a single .pfx PKCS#12 certificate file. The controller will accept the PEM/DER file as long as the format of the private key and certificate are valid.
PEM-formatted CA public certificate file	If you choose to install this optional certificate, you must do so when specifying the PCKCS#12 or PEM/DER certificates.



Note

When generating the PKCS#12 certificate file or PEM/DER certificate and key files, you must ensure that the interface identified in the certificate corresponds to the controller's interface for which the certificate is being installed.

- 2 Understand how the controller monitors the expiration date of installed certificates.

The controller generates an entry in the events information log as the certificate expiry date approaches, based on the following schedule: 15, 8, 4, 2, and 1 day prior to expiration. The log messages cease when the certificate expires. For more information, refer to the Extreme Networks ExtremeWireless *Maintenance Guide*.

- 3 Understand how the controller manages certificates during upgrades and migrations.

Installed certificates will be backed up and restored with the controller configuration data. Installed certificates will also be migrated during an upgrade and during a migration.

Installing a Certificate for a Controller Interface

To install a certificate for a Controller Data Interface:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Network** > **Topologies**. The **Topologies** tab is displayed.

- 3 Click the **Certificates** tab. Topologies with an L3 interface will be listed.
- 4 In the **Interface Certificates** table, click to select the topology for which you want to install a certificate.

The **Configuration for Topologies** section displays.



Note

There are separate certificates if IPv4 and IPv6 is configured for Admin topology.

The Configuration for Topologies section and the Generate Signing Request button become available. Use the field and button descriptions in [Table 8](#) to create and install certificates.



Note

The certificate Common Name (CN) must match the interface IP or DNS addresses (Admin only).

Topologies

Topology	Expiry Date	CA Cert.	Name (CN)	Org. Unit (OU)	Organization (O)
Admin	-	-	-	-	-
BAC	-	-	-	-	-
BAC2	-	-	-	-	-
PHY1	-	-	-	-	-

Configuration for Topology BAC

- Replace/Install selected Topology's certificate
- Replace/Install selected Topology's certificate and key from a single file
- Replace/Install selected Topology's certificate and key from separate files
- Reset selected Topology to the factory default certificate and key
- No change

Generate Signing Request

Table 8: Topologies Page: Certificates Tab Fields and Buttons

Field/Button	Description
Interface Certificates	
Topology	Topology name
Expiry Date	Date when the certificate expires



Table 8: Topologies Page: Certificates Tab Fields and Buttons (continued)

Field/Button	Description
CA Cert.	Identifies whether or not a CA certificate has been installed on the topology.
Name (CN)	The IP address of DNS address associated with the topology that the certificate applies to. Note: The Name field supports both IPv4 or IPv6 addresses.
Org Unit (OU)	Name of the organization's unit.
Organization	Name of the organization
Configuration for Topology	
Replace/Install selected Topology's certificate	<p>To replace/install the existing port's certificate and key using this option, do the following:</p> <ol style="list-style-type: none"> 1 From the click the Generate Signing Request button to create the certificate and key. 2 Download the CSR when prompted. 3 Use a 3rd party certificate service to sign the CSR and create a certificate and a Certificate Authority (CA) file. 4 Save the certificate on your computer. 5 Return to the Certificates tab on the ExtremeWireless UI. 6 Select the topology for which you created the certificate and select Replace/Install selected Topologies certificate. 7 Click Browse next to the Signed certificate to install field. 8 Navigate to the certificate file you want to install for this port, and then click Open. The certificate file name is displayed in the Certificate file to install field. 9 (Optional) Click Browse next to the Optional:Enter PEM-encoded CA public certificates file field. The Choose file dialog is displayed. 10 (Optional) Navigate to the certificate file you want to install for this port, and then click Open. The certificate file name is displayed in the Optional:Enter PEM-encoded CA public certificates file field. <p>Note: If you choose to install a CA public certificate, you must install it when you install the PEM/DER certificate and key.</p>

Table 8: Topologies Page: Certificates Tab Fields and Buttons (continued)

Field/Button	Description
Replace/Install selected Topology's certificate and key from a single file	<p>To replace the existing port's certificate and key using this option, do the following:</p> <ol style="list-style-type: none"> 1 Click Browse next to the PKCS #12 file to install field. The Choose file dialog is displayed. 2 Navigate to the certificate file you want to install for this port, and then click Open. The certificate file name is displayed in the PKCS #12 file to install field. 3 In the Private key password box, type the password for the key file. The key file is password protected. 4 (Optional) Click Browse next to the Optional:Enter PEM-encoded CA public certificates file field. The Choose file dialog is displayed. 5 (Optional) Navigate to the certificate file you want to install for this port, and then click Open. The certificate file name is displayed in the Optional:Enter PEM-encoded CA public certificates file field. <p>Note: If you choose to install a CA public certificate, you must install it when you install the PEM/DER certificate and key.</p>
Replace/Install selected Topology's certificate and key from separate files	<p>To replace the existing port's certificate and key using this option, do the following:</p> <ol style="list-style-type: none"> 1 Click Browse next to the PKCS #12 file to install field. The Choose file dialog is displayed. 2 Navigate to the certificate file you want to install for this port, and then click Open. The certificate file name is displayed in the PKCS #12 file to install field. 3 Click Browse next to the Private key file to install field. The Choose file dialog is displayed. 4 Navigate to the key file you want to install for this port, and then click Open. The key file name is displayed in the Private key file to install field. 5 In the Private key password box, type the password for the key file. The key file is password protected. 6 (Optional) Click Browse next to the Optional:Enter PEM-encoded CA public certificates file field. The Choose file dialog is displayed. 7 (Optional) Navigate to the certificate file you want to install for this port, and then click Open. The certificate file name is displayed in the Optional:Enter PEM-encoded CA public certificates file field. <p>Note: If you choose to install a CA public certificate, you must install it when you install the PEM/DER certificate and key.</p>
Reset selected Topology to the factory default certificate and key	Remove custom certificate that user installed.
No change	No change.

Table 8: Topologies Page: Certificates Tab Fields and Buttons (continued)

Field/Button	Description
Generate Signing Request	To generate a CSR for the controller, click Generate Signing Request. The Generate Certificate Signing Request window displays (Figure 10).
Save	Click to save the changes to this Topology.



Note

To avoid the certificate-related web browser security warnings when accessing the Wireless Assistant, you must also import the customized certificates into your web browser application.

Figure 10: Generate Certificate Signing Request Window

Table 9: Generate Certificate Signing Request Page - Fields and Buttons

Field/Button	Description
Country name	The two-letter ISO abbreviation of the name of the country
State or Province name	The name of the State/Province
Locality name (city)	The name of the city.
Organization name	The name of the organization
Organizational Unit name	The name of the unit within the organization.
Common Name	Set the common name to be one of the following: the IP address of the interface that the CSR applies to. a DNS address associated with the IP address of the interface that the CSR applies to.

Table 9: Generate Certificate Signing Request Page - Fields and Buttons (continued)

Field/Button	Description
Email address	The email address of the organization
Generate Signing Request	Click to generate a signing request. A certificate request file is generated (.csr file extension). The name of the file is the IP address of the topology you created the CSR for. The File Download dialog is displayed.

Configuring the Login Authentication Mode

You can configure the following login authentication modes to authenticate administrator login attempts:

- Local authentication — The controller uses locally configured login credentials and passwords. See [Configuring the Local Login Authentication Mode and Adding New Users](#) on page 75.
- RADIUS authentication — The controller uses login credentials and passwords configured on a RADIUS server. See [Configuring the RADIUS Login Authentication Mode](#) on page 78.
- Local authentication first, then RADIUS authentication — The controller first uses locally configured login credentials and passwords. If this login fails, the controller attempts to validate login credentials and passwords configured on a RADIUS server. See [Configuring the Local, RADIUS Login Authentication Mode](#) on page 82.
- RADIUS authentication first, then local authentication — The controller first uses login credentials and passwords configured on a RADIUS server. If this login fails, the controller attempts to validate login credentials and passwords configured locally. See [Configuring the RADIUS, Local Login Authentication Mode](#) on page 84.



Note

The ExtremeWireless Appliance enables you to recover the controller via the Rescue mode if you have lost its login password. For more information, see the *ExtremeWireless Maintenance Guide*.

Configuring the Local Login Authentication Mode and Adding New Users

Local login authentication mode is enabled by default. If the login authentication was previously set to another authentication mode, you can change it to the local authentication. You can also add new users and assign them to a login group — as full administrators, read-only administrators, or as a GuestPortal managers. For more information, see [Defining Wireless Assistant Administrators and Login Groups](#) on page 673.

To configure the local login authentication mode:

- 1 From the top menu, click **Controller**.

- In the left pane, click **Administration** > **Login Management**.
The **Login Management** screen displays.

- In the Authentication mode section, click **Configure**.
The **Login Authentication Mode Configuration** window is displayed.

Enable	Authentication
<input checked="" type="checkbox"/>	Local
<input type="checkbox"/>	RADIUS

- 4 Select the **Local** check box.
If the RADIUS check box is selected, deselect it.
- 5 Click **OK**.
- 6 In the **Add User** section, select one of the following from the **Group** drop-down list:
 - **Full Administrator** — Grants the administrator's access rights to the administrator.
 - **Read-only Administrator** — Grants read-only access right to the administrator.
 - **GuestPortal Manager** — Grants the user GuestPortal manager rights.
- 7 In the **User ID** box, type the user's ID.
- 8 In the **Password** box, type the user's password.

**Note**

UNICODE characters are not supported in passwords for local and remote RADIUS/TACACS+ authentication. All passwords must be 8 to 24 characters long.

- 9 In the **Confirm Password** box, re-type the password.
- 10 To add the user, click **Add User**. The new user is added.
- 11 Click **Save**.

The **Administrator Password Confirmation** window is displayed.

- 12 Select the appropriate option.
 - **Yes** — Change authentication mode to local. Use the administrator password currently defined on the controller.
 - **Yes, but I want to change administrator's password first** — Change authentication mode to local and change the administrator password currently defined on the controller.
 - **No** — Do not change the authentication mode to local.
- 13 Click **Submit**.
- 14 If you chose **Yes, but I want to change administrator's password first**, you are prompted to change the administrator's password.

Configuring the RADIUS Login Authentication Mode

The local login authentication mode is enabled by default. You can change the local login authentication mode to RADIUS-based authentication.

**Note**

Before you change the default local login authentication to RADIUS-based authentication, you must configure the RADIUS Server on the **Global Settings** screen. For more information, see [VNS Global Settings](#) on page 392.

RADIUS is a client/server authentication and authorization access protocol used by a network access server (NAS) to authenticate users attempting to connect to a network device. The NAS functions as a client, passing user information to one or more RADIUS servers. The NAS permits or denies network access to a user based on the response it receives from one or more RADIUS servers. RADIUS uses User Datagram Protocol (UDP) for sending the packets between the RADIUS client and server.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one configured on the RADIUS servers. The RADIUS clients and servers use the key to encrypt all RADIUS packets transmitted. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never transmitted over the network.

Note

Before you configure the system to use RADIUS-based login authentication, you must configure the Service-Type RADIUS attribute on the RADIUS server.



EWC uses the standard RADIUS attribute `Service-Type` to put the user into the appropriate groups:

- Administrator Service-Type = 6
- Read-Only Service-Type = 7
- GuestPortal Manager Service-Type = 8

To configure the RADIUS login authentication mode:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Administration** > **Login Management**. The **Login Management** screen displays.

- 3 Click the **RADIUS Authentication** tab.

The screenshot displays the configuration interface for the ExtremeWireless Appliance, specifically the **RADIUS Authentication** tab. The interface is divided into two main sections: **Local Authentication** and **RADIUS Authentication**.

Local Authentication: This section includes a dropdown menu for **NAC** with a **Use** button. Below it is a **Configured Servers** list containing the server ID **1234**, with **Up** and **Down** buttons for management. At the bottom of this section are **Test** and **View Summary** buttons.

RADIUS Authentication: This section features a **Auth *** section with a checked **Use server for Authentication** option. Below this, there are input fields for **NAS IP Address** (172.20.46.10), **NAS identifier** (EWC), and **Auth. type** (CHAP). A **Reset** button is located at the bottom right of this section.

At the bottom of the interface, the **Authentication mode:** is set to **Local**. To the right of this mode indicator are **Configure** and **Save** buttons. A large grey arrow points from the **Configure** button towards the text in step 4.

- 4 In the **Authentication mode** section, click **Configure**.
The Login Authentication Mode Configuration window is displayed.

- 5 Deselect **Local** and select the **RADIUS** check box.

Login Authentication Mode Configuration ? X

Each enabled authentication method will be tried in order from the top of the list to the bottom. The process stops when an authentication method successfully authenticates the credentials or all enabled authentication methods failed to authenticate the credentials.

Enable	Authentication
<input type="checkbox"/>	Local
<input checked="" type="checkbox"/>	RADIUS

Move Up
Move Down

OK Cancel

- 6 Click **OK**.
- 7 From the drop-down list, located next to the **Use** button, select the RADIUS Server that you want to use for the RADIUS login authentication, and then click **Use**. The RADIUS Server's name is displayed in the **Configured Servers** box, and in the **Auth** section, and the following default values of the RADIUS Server are displayed.



Note

The RADIUS Servers displayed in the list located against the **Use** button are defined on **Global Settings** screen. For more information, see [VNS Global Settings](#) on page 392.

The following values can be edited:

- **NAS IP address** — The IP address of Network Access Server (NAS).
 - **NAS Identifier** — The Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers, and then acting on the response returned.
 - **Auth Type** — The authentication protocol type (PAP, CHAP, MS-CHAP, or MS-CHAP2).
 - **Set as Primary Server** — Specifies the primary RADIUS server when there are multiple RADIUS servers.
- 8 To add additional RADIUS servers, repeat step 7.



Note

You can add up to three RADIUS servers to the list of login authentication servers. When you add two or more RADIUS servers to the list, you must designate one of them as the Primary server. The controller first attempts to connect to the Primary server. If the Primary Server is not available, it tries to connect to the second and third server according to their order in the **Configured Servers** box. You can change the order of RADIUS servers in the **Configured Servers** box by clicking on the Up and **Down** buttons.

- 9 Click **Test** to test connectivity to the RADIUS server.

Note

You can also test the connectivity to the RADIUS server after you save the configuration. If you do not test the RADIUS server connectivity, and you have made an error in configuring the RADIUS-based login authentication mode, you will be locked out of the controller when you switch the login mode to the RADIUS login authentication mode. If you are locked out, access Rescue mode via the console port to reset the authentication method to local.

The following window is displayed.

The screenshot shows a dialog box titled "Test RADIUS Servers" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields. The first is labeled "User ID:" and the second is labeled "Password:". Below these fields are two buttons: "Test" and "Cancel".

- 10 In the **User ID** and the **Password** fields, type the user's ID and the password, which were configured on the RADIUS Server, and then click **Test**.

The RADIUS connectivity result is displayed.

Note

To learn how to configure the User ID and the Password on the RADIUS server, refer to your RADIUS server's user guide.

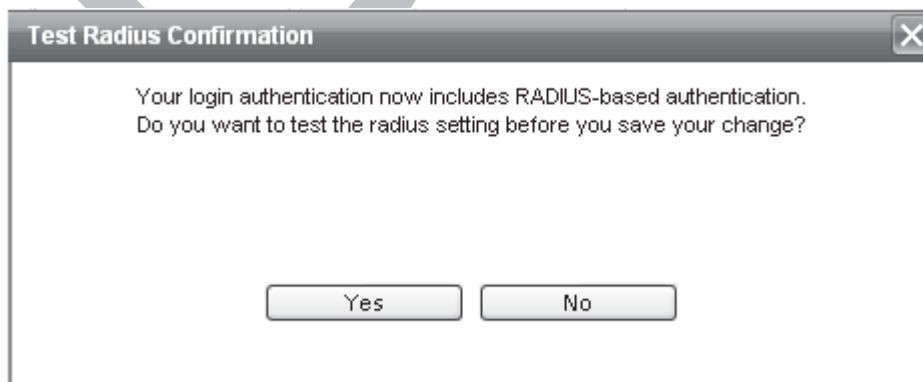
The screenshot shows the same "Test RADIUS Servers" dialog box, but now it displays the results. The text "RADIUS Test Results:" is followed by "Successful". At the bottom center of the dialog, there is a "Close" button.

If the test is not successful, the following message will be displayed:



- 11 If the RADIUS connectivity test displays “Successful” result, click **Save** on the RADIUS Authentication screen to save your configuration.

The following window is displayed:



- 12 If you tested the RADIUS server connectivity earlier in this procedure, click **No**. If you click **Yes**, you will be asked to enter the RADIUS server user ID and password.
- 13 To change the authentication mode to RADIUS authentication, click **OK**.
You will be logged out of the controller immediately. You must use the RADIUS login user name and password to log on the controller.

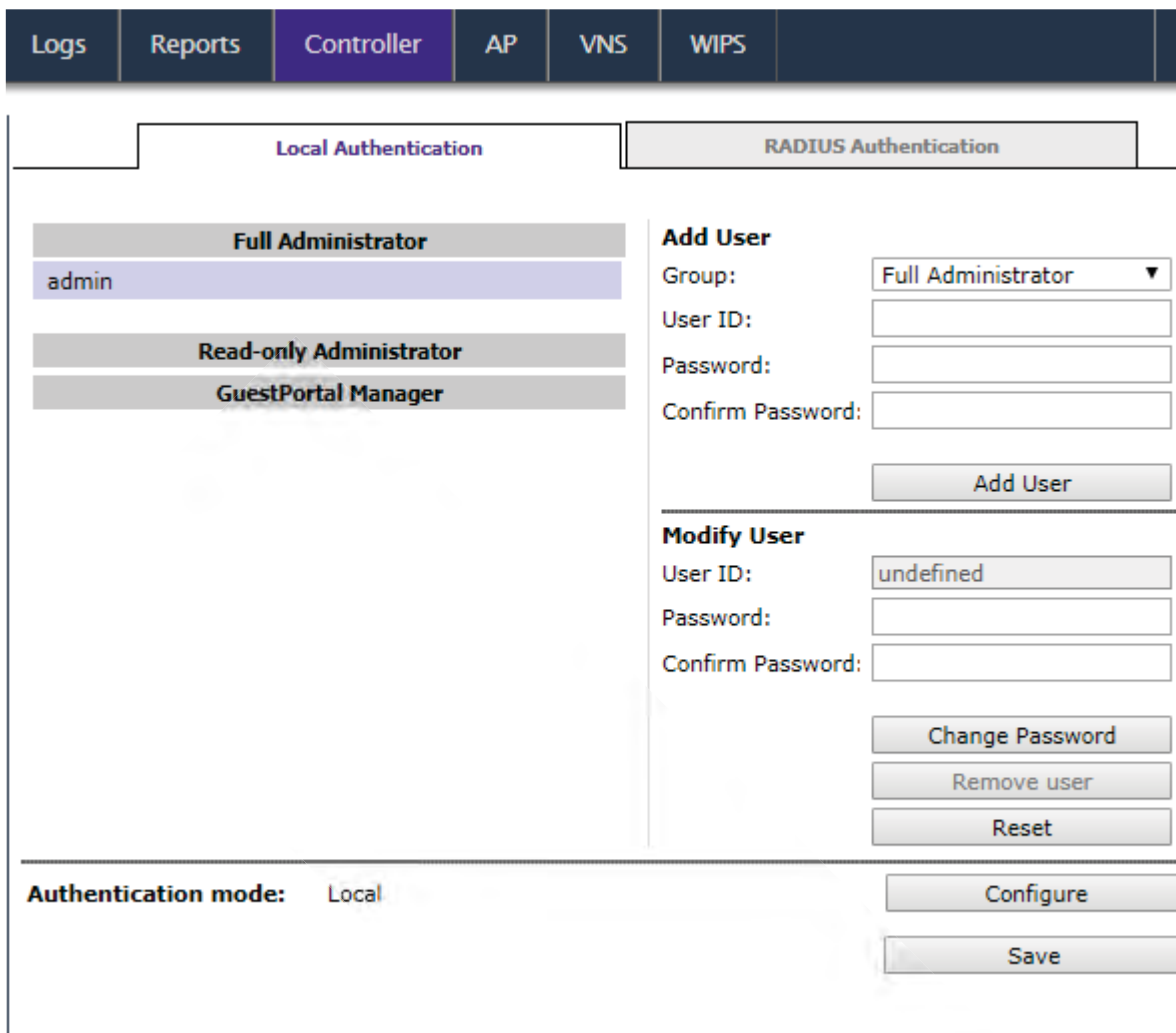
To cancel the authentication mode changes, click **Cancel**.

Configuring the Local, RADIUS Login Authentication Mode

To configure the Local, RADIUS login authentication mode:

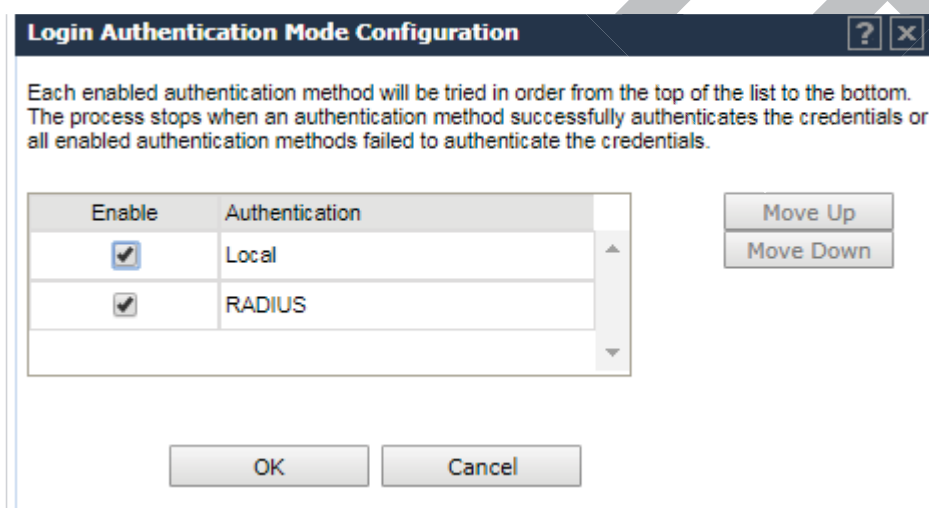
- 1 From the top menu, click **Controller**.

2 In the left pane, click **Administration** > **Login Management**. The Login Management screen displays.



3 In the **Authentication mode** section, click **Configure**.

4 Select the **Local** and **RADIUS** check box.



- 5 If necessary, select **Local** and use the **Move Up** button to move **Local** to the top of the list.
- 6 Click **OK**.
- 7 On the **Login Management** screen, click **Save**.

For information on setting local login authentication settings, see [Configuring the Local Login Authentication Mode and Adding New Users](#) on page 75.

For information on setting RADIUS login authentication settings, see [Configuring the RADIUS Login Authentication Mode](#) on page 78.

Configuring the RADIUS, Local Login Authentication Mode

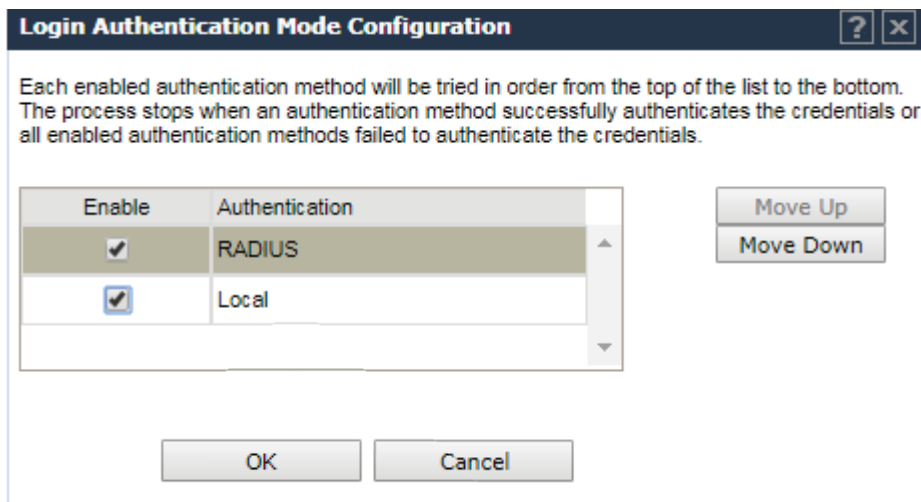
To configure the RADIUS, Local login authentication mode:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Administration** > **Login Management**. The **Login Management** screen displays.

The screenshot shows the 'Login Management' interface. The top navigation bar has 'Controller' selected. The left pane shows 'Administration' > 'Login Management'. The main content area has two tabs: 'Local Authentication' (selected) and 'RADIUS Authentication'. Under 'Local Authentication', there are three user roles: 'Full Administrator', 'Read-only Administrator', and 'GuestPortal Manager'. The 'Full Administrator' role has a user named 'admin' listed below it. To the right, there are sections for 'Add User' and 'Modify User'. The 'Add User' section has fields for Group (set to 'Full Administrator'), User ID, Password, and Confirm Password, with an 'Add User' button below. The 'Modify User' section has fields for User ID (set to 'undefined'), Password, and Confirm Password, with buttons for 'Change Password', 'Remove user', and 'Reset'. At the bottom, the 'Authentication mode' is set to 'Local', and there are 'Configure' and 'Save' buttons.

- 3 In the **Authentication mode** section, click **Configure**.
The **Login Authentication Mode Configuration** window is displayed.
- 4 Select the **Local** and **RADIUS** check box.

- If necessary, select the **RADIUS** field and use the **Move Up** button to move **RADIUS** to the top of the list.



- Click **OK**.
- On the **Login Management** screen, click **Save**.

For information on setting RADIUS login authentication settings, see [Configuring the RADIUS Login Authentication Mode](#) on page 78.

For information on setting local login authentication settings, see [Configuring the Local Login Authentication Mode and Adding New Users](#) on page 75.

Configuring SNMP

The controller supports the *SNMP* for retrieving statistics and configuration information. If you enable SNMP on the controller, you can choose either SNMPv3 or SNMPv1/v2 mode. If you configure the controller to use SNMPv3, then any request other than SNMPv3 request is rejected. The same is true if you configure the controller to use SNMPv1/v2.

To configure SNMP:

- From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.

- 2 In the left pane, click **Network** > **SNMP**.

The **SNMP** screen displays.

SNMP Common Settings

Mode: No SNMP SNMPv1/v2c SNMPv3

Contact Name:

Location:

SNMP Port:

Forward Traps:

Publish AP as interface of controller:

SNMPv1/v2c | **SNMPv3**

Read Community Name:

Read/Write Community Name:

Manager A:

Manager B:

- 3 In the SNMP Common Settings section, configure the following:
- **Mode** — Select **SNMPv1/v2c** or **SNMPv3** to enable SNMP.
 - **Contact Name** — The name of the SNMP administrator.
 - **Location** — The physical location of the controller running the SNMP agent.
 - **SNMP Port** — The destination port for the SNMP traps. Possible ports are 0–65555.
 - **Forward Traps** — The lowest severity level of SNMP trap that you want to forward.
 - **Publish AP as interface of controller** — Enable or disable SNMP publishing of the access point as an interface to the controller.
- 4 Select the tab for the SNMP version you are configuring. For more information, see:
- [Configuring SNMPv1/v2c-specific Parameters](#) on page 87
 - [Configuring SNMPv3-specific Parameters](#) on page 87

Configuring SNMPv1/v2c-specific Parameters

- 1 Configure the following parameters on the **SNMPv1/v2c** tab:
 - **Read Community Name** — The password that is used for read-only *SNMP* communication.
 - **Read/Write Community Name** — The password that is used for write *SNMP* communication.
 - **Manager A** — The IP address of the server used as the primary network manager that will receive *SNMP* messages.
 - **Manager B** — The IP address of the server used as the secondary network manager that will receive *SNMP* messages.



Note

Manager A and Manager B address fields support both IPv4 or IPv6 addresses.

- 2 Click **Save**.

Configuring SNMPv3-specific Parameters

- 1 Configure the parameters following on the **SNMPv3** tab:
 - **Context String** — A description of the *SNMP* context.
 - **Engine ID** — The *SNMPv3* engine ID for the controller running the *SNMP* agent. The engine ID must be from 5 to 32 characters long.
 - **RFC3411 Compliant** — The engine ID will be formatted as defined by `SnmEngineID` textual convention (that is, the engine ID will be prepended with *SNMP* agents' private enterprise number assigned by IANA as a formatted HEX text string).
- 2 Click **Add User Account**. The **Add SNMPv3 User Account** window displays.
- 3 Configure the following parameters:
 - **User** — Enter the name of the user account.
 - **Security Level** — Select the security level for this user account. Choices are: `authPriv`, `authNoPriv`, `noAuthnoPriv`.
 - **Auth Protocol** — If you have selected a security level of `authPriv` or `authNoPriv`, select the authentication protocol. Choices are: *MD5 (Message-Digest algorithm 5)*, `SHA`, `None`.
 - **Auth Password** — If you have selected a security level of `authPriv` or `authNoPriv`, enter an authentication password.
 - **Privacy Protocol** — If you have selected the security level of `authPriv`, select the privacy protocol. Choices are: `DES`, `None`.
 - **Privacy Password** — If you have selected the security level of `authPriv`, enter a privacy password.
 - **Engine ID** — If desired, enter an engine ID. The ID can be between 5 and 32 bytes long, with no spaces, control characters, or tabs.
 - **Destination IP** — If desired, enter the IP address of a trap destination.



Note

The Destination IP address field supports both IPv4 or IPv6 addresses.

- 4 Click **OK**. The **Add SNMPv3 User Account** window closes.
- 5 Repeat steps 2 through 4 to add additional users.

- 6 In the **Trap 1** and **Trap 2** sections, configure the following parameters:
 - **Destination IP** – The IP address of the machine monitoring SNMPv3 traps

**Note**

The Destination IP address field supports both IPv4 or IPv6 addresses.

- **User Name** – The SNMPv3 user to configure for use with SNMPv3 traps
- 7 Click **Save**.

Editing an SNMPv3 User

To edit an SNMPv3 user:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **SNMP**. The **SNMP** screen displays.
- 3 Click the **SNMPv3** tab.
- 4 Select an SNMP user.
- 5 Click **Edit Selected User**. The **Edit SNMPv3 User Account** window displays.
- 6 Edit the user configuration as desired.
- 7 Click **OK**. The **Edit SNMPv3 User Account** window closes.
- 8 Click **Save**.

Deleting an SNMPv3 User

To delete an SNMPv3 user:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **SNMP**. The **SNMP** screen displays.
- 3 Click the **SNMPv3** tab.
- 4 Select an SNMP user.
- 5 Click **Delete Selected User**. You are prompted to confirm that you want to delete the selected user.
- 6 Click **OK**.

SNMP Trap Types

The SNMP agent generates traps to notify the administrator of events such as configuration changes, component failures, and disconnection of Access Points. Administrators can configure the Agent and the Controller, defining the level of trap to receive. The following trap types are supported by ExtremeWireless Controllers:

- Interfaces MIB (IF-MIB) linkDown (.1.3.6.1.6.3.1.1.5.3)
- Interfaces MIB (IF-MIB) linkUp (.1.3.6.1.6.3.1.1.5.4)
- HIPATH-WIRELESS-HWC-MIB apTunnelAlarm (.1.3.6.1.4.1.4329.15.3.19.4)
 - Sent by the controller when it detects that it has lost the connection to an AP. The trap identifies the AP that the controller can no longer contact.
- HIPATH-WIRELESS-HWC-MIB hiPathWirelessLogAlarm (.1.3.6.1.4.1.4329.15.3.9.6)

- A generic trap that contains specific information relevant to the event. The information is carried in the trap, and the information varies from event to event.
- The trap contains the trap severity, the component on the controller that raised the event, and the text string associated with the event, as it appears in the controller GUI.
- A trap containing one event that also is displayed in the controller's Event / Log report page. The trap is sent when the event is raised and recorded on the controller.
- This trap accounts for the vast majority of traps messages sent by the controller at most sites.

Configuring Network Time

You should synchronize the clocks of the controller and the APs to ensure that the logs and reports reflect accurate time stamps. For more information, see [Working with Reports and Statistics](#) on page 621.

The normal operation of the controller will not be affected if you do not synchronize the clock. The clock synchronization is necessary to ensure that the logs display accurate time stamps. In addition, clock synchronization of network elements is a prerequisite for the following configuration:

- Mobility Manager
- Session Availability

Network Time Synchronization

Network time is synchronized in one of two ways:

- Using the system's time — The system's time is the controller's time.
- Using Network Time Protocol (NTP) — The Network Time Protocol is a protocol for synchronizing the clocks of computer systems over packet-switched data networks.

The controller automatically adjusts for any time change due to Daylight Savings time.

Configuring the Network Time Using the System's Time

- 1 From the top menu, click **Controller**.

- In the left pane, click **Network** > **Network Time**. The **Network Time** screen displays.

Network Time

Time Zone Settings*

Continent or Ocean:

Time Zone Region:

*Time Zone changes may take up to 60 seconds to take effect

System Time (mm-dd-yyyy hh:mm)

NTP

- From the **Continent or Ocean** drop-down list, click the appropriate large-scale geographic grouping for the time zone.
- From the **Time Zone Region** drop-down list, click the appropriate time zone region for the selected country.
- Click **Apply Time Zone**.
- In the **System Time** field, type the system time.
- Click **Set Clock**. The WLAN network time is synchronized in accordance with the controller's time.

Configuring the Network Time Using an NTP Server

- From the top menu, click **Controller**.

- 2 In the left pane, click **Network** > **Network Time**. The **Network Time** screen displays.

Network Time

Time Zone Settings*

Continent or Ocean:

Time Zone Region:

*Time Zone changes may take up to 60 seconds to take effect

System Time (mm-dd-yyyy hh:mm)

NTP

Time Server 1:

Time Server 2:

Time Server 3:

Run local NTP Server

- 3 From the **Continent or Ocean** drop-down list, click the appropriate large-scale geographic grouping for the time zone.
- 4 From the **Time Zone Region** drop-down list, click the appropriate time zone region for the selected country.
- 5 Click **Apply Time Zone**.
- 6 In the **System Time** box, type the system time.
- 7 Select the **Use NTP** check box.



Note

If you want to use the controller as the NTP Server, select the **Run local NTP Server** check box, and click **Apply**.

- 8 In the **Time Server 1** text box, type the IP address or FQDN (Full Qualified Domain Name) of an NTP time server that is accessible on the enterprise network.



Note

The Time Server fields supports both IPv4 and IPv6 addresses.

- 9 Repeat for **Time Server2** and **Time Server3** text boxes.
If the system is not able to connect to the Time Server 1, it will attempt to connect to the additional servers that have been specified in Time Server 2 and Time Server 3 text boxes.

10 Click **Apply**. The WLAN network time is synchronized in accordance with the specified time server.

Configuring Secure Connections

The controllers communicate amongst themselves using a secure protocol. Among other things, this protocol is used to share between controllers the data required for high availability. They also use this protocol to communicate with NMS Wireless Manager. The protocol requires the use of a shared secret for mutual authentication of the end points.

By default the controllers and NMS Wireless Manager use a well known factory default shared secret. This makes it easy to get up and running but is not as secure as some sites require.

The controllers and NMS Wireless Manager allow the administrator to change the shared secret used by the secure protocol. In fact the controllers and Wireless Manager can use a different shared secret for each individual end point to which they connect with the protocol.

To configure the shared secret for a connection on the controller:

- 1 From the top menu, click **Controller**.

- In the left pane, click **Network** > **Secure Connections**.

The **Secure Connections** screen displays.

Shared Secret for Remote Connections

Enable Weak Ciphers

Peer IP Address	Shared Secret
<input type="text"/>	<input type="text"/>

- Select **Enable Weak Ciphers** to enable weak ciphers for the remote connections. Disabling weak ciphers prevents users from accessing various web pages on the controller using less secure methods.
- Enter the Server IP address of the other end of the secure protocol tunnel and the shared secret to use.
- Click **Add/Update**.
- Click **Save**.



Note

Configure the same shared secret onto the devices at each end of the connection. Otherwise, the two controllers or controller and NMS Wireless Manager will not be able to communicate.

Configuring DNS Servers for Resolving Host Names of NTP and RADIUS Servers

Because the **Global Settings** screen allows you to set up NTP and RADIUS servers by defining their host names, you have to configure your DNS servers to resolve the host names of NTP and RADIUS servers to the corresponding IP addresses. Go to **VNS > Global Settings**.



Note

For more information on RADIUS server configuration, see [Defining RADIUS Servers and MAC Address Format](#) on page 394.

You can configure up to three DNS servers to resolve NTP and RADIUS server host names to their corresponding IP addresses.

The controller sends the host name query to the first DNS server in the stack of three configured DNS servers. The DNS server resolves the queried domain name to an IP address and sends the result back to the controller.

If for some reason, the first DNS server in the stack of configured DNS servers is not reachable, the controller sends the host name query to the second DNS server in the stack. If the second DNS server is also not reachable, the query is sent to the third DNS server in the stack.

To configure DNS servers for resolving host names of NTP and RADIUS servers:

- 1 From the top menu, click **Controller**.

- In the left pane, click **Administration** > **Host Attributes**.

The **Host Attributes** screen displays.

Host Attributes

Network Identification

Host Name:

Domain Name:

DNS

Server Address:

Default Gateway IP:

- In the DNS box, type the DNS server's IP address in the **Server Address** field and then click **Add Server**. The new server is displayed in the DNS servers' list.



Note

You can configure up to three DNS servers. The Server Address field supports both IPv4 and IPv6 addresses.

- In the **Default Gateway IP** box, enter the IP address of the Default Gateway.
- To save your changes, click **Save**.

Using a Third-party Location-based Solution

ExtremeWireless supports the following location-based solutions:

- AeroScout
- Ekahau
- Centrak

On the controller, configure the AeroScout/Ekahau/Centrak server IP address and enable the location-based service. When using AeroScout or Ekahau, the location-based server is aware of the controller IP address. And if using AeroScout, the controller notifies the AeroScout server of the operational APs.

Enable the location-based service on the APs that you want to participate.

**Note**

Participating APs must use the 2.4 GHz band and the radio that receives location-based service tags must have at least one WLAN service associated with it.

Once you have enabled the location-based service on the controller and the participating APs, at least one of the participating APs will receive reports from a location-based service Wi-Fi RFID tag in the 2.4 GHz band. The tag reports are collected by the AP and forwarded to the location-based server by encapsulating the tag reports in a WASSP tunnel and routing them as IP packets through the controller. When using Ekahau or Centrak, the controller does not converse directly with the location-based service server.

**Note**

Tag reports are marked with UP=CS5, and DSCP = 0xA0. On the wireless controller, tag reports are marked with UP=CS5 to the core (if 802.1p exists).

An AP's tag report collection status is reported in the AP Inventory report. For more information, see [Viewing Routing Protocol Reports](#) on page 657.

If availability is enabled, tag report transmission pauses on failed over APs until they are configured and notified by the location-based server. With an availability pair, it is good practice to configure both controllers with the same location-based service.

When location-based service support is disabled on the controller, the controller does not communicate with the location-based server and the APs do not perform any location-based functionality.

Ensure that your location-based service tags are configured to transmit on all non-overlapping channels (1, 6 and 11) and also on channels above 11 for countries where channels above 11 are allowed. For information about proper deployment of the location-based solution, refer to the third-party documentation (AeroScout/Ekahau/Centrak).

Related Links

[Configuring Location-Based Services](#) on page 96

[AP Multi-Edit Properties](#) on page 111

[AP Properties Tab - Advanced Settings](#) on page 164

Configuring Location-Based Services

To configure a controller for use with an AeroScout/Ekahau/Centrak solution:

- 1 From the top menu, click **Controller**.

- 2 In the left pane, click **Services** > **Location-based Service**.

The screenshot shows the configuration page for Location-based Service. The left navigation pane has the following items: Administration, Logs, Network, Services (highlighted), Location-based Service (highlighted), and Mobility Manager. The main content area is titled "Location-based Service" and contains a dropdown menu with the following options: Ekahau, Disabled, Aeroscout, Ekahau, and Centrak. Below the dropdown are three input fields: the first is labeled ".4", the second is labeled "8", and the third is labeled "Multicast Address: 01:18:8E:00:00:00".

- 3 Select the desired location-based service for the controller.
- Enter the IP address of the location based service server.
 - Centrak and Ekahau configuration offer a default port number and multicast address, but you can modify the default values if necessary.
- 4 Click **Save**.
- Now assign APs to participate in the location-based service.

- From the top menu, click **AP**. In the left pane, click **APs**.

Note



You can enable location-based service on APs using the **Location-based service field** on the **AP Multi-edit** screen and the **Advanced** window of the **AP Default Settings** screen. The following procedure shows you how to enable location-based services on one AP at a time.

<input type="checkbox"/>	Name ▲	Model ◆	Site ◆	Location ◆	SW Version ◆	Status ◆
<input type="checkbox"/>	14300167085D0000	AP3825e			10.41.02.0002T	Foreign
<input type="checkbox"/>	1548Y-1007900000	AP3965i-ROW	s1		10.41.01.0075T	Local
<input type="checkbox"/>	3916	AP3916ic-ROW			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3715i	AP3715i			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3765i	AP3765i			10.41.02.0002T	Local
<input type="checkbox"/>	AP3912i-ROW-1	AP3912i-ROW			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3915	AP3915e-ROW			10.41.02.0002T	Local
<input type="checkbox"/>	Dual band	AP3765e			10.41.02.0002T	Local
<input type="checkbox"/>	W786	W786C-2IA-RJ45			10.41.02.0002T	Foreign
<input type="checkbox"/>	W788	W788C-2-RJ45			10.41.02.0002T	Local

Showing: 10 rows, Local: 5, Foreign: 5

- Click on an AP row.
The **AP Status** dashboard displays.
- Click **Configure** to display the **Configuration** dialog.

- 8 Click **Advanced**.

The **Advanced** dialog displays.

Advanced

Poll Timeout: 15 seconds

Secure Tunnel: Disabled

Enable SSH Access

Enable location-based service

Maintain client sessions in event of poll failure

Restart service in the absence of controller

Use broadcast for disassociation

Enable LLDP

IP Multicast Assembly

Balanced Channel List Power

Low Power Mode Override *

* This setting may cause AP to reboot.

LED: Normal

Real Capture: Start 300 seconds

Close

- 9 Select **Enable location-based service** and close the dialog.
- 10 Enable Location-based services on each additional AP that you want to participate.
- 11 Click **Save**.

Related Links

[Using a Third-party Location-based Solution](#) on page 95

[AP Multi-Edit Properties](#) on page 111

[AP Properties Tab - Advanced Settings](#) on page 164

Additional Ongoing Operations of the System

Ongoing operations of the Extreme Networks ExtremeWireless system can include the following:

- Controller System Maintenance
- Client Disassociate
- Logs and Traces
- Reports and Displays

For more information, see [Performing System Administration](#) on page 669 or the Extreme Networks *ExtremeWireless Maintenance Guide*.

Draft

4 Configuring the ExtremeWireless APs

Wireless AP Overview
Discovery and Registration
Viewing a List of All APs
Wireless AP Default Configuration
Configuring Wireless AP Properties
Outdoor Access Point Installation
Assigning Wireless AP Radios to a VNS
Configuring Wireless AP Radio Properties
Configuring IoT Applications
Setting Up the Wireless AP Using Static Configuration
Setting Up 802.1x Authentication for a Wireless AP
Configuring Co-Located APs in Load Balance Groups
Configuring an AP Cluster
Configuring an AP as a Guardian
Configuring a Captive Portal on an AP
AP3916ic Integrated Camera Deployment
Performing AP Software Maintenance
Understanding the ExtremeWireless LED Status

Wireless AP Overview

Extreme Networks ExtremeWireless APs use the 802.11 wireless standards (802.11a/b/g/n/ac) for network communications, and bridge network traffic to an Ethernet LAN. In addition to the Wireless APs that run proprietary software and communicate with a controller only, Extreme Networks offers a Cloud-enabled APs. The 3805i and the AP39xx series are radar capable, Cloud-enabled APs that interoperate fully with ExtremeCloud and other ExtremeWireless products.

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

A UDP-based protocol enables communication between an AP and a controller. The UDP-based protocol encapsulates IP traffic from the AP and directs it to the controller. The controller decapsulates the packets and routes them to the appropriate destinations, while managing sessions and applying roles.

AP Model Firmware Support

Refer to the [ExtremeWireless Hardware Firmware Support Matrix](#) to easily determine the currently supported firmware version and the minimum firmware version for each ExtremeWireless access point.

Wireless Protocol Standards (802.11)

Most current wireless networks and end-user devices use the IEEE 802.11n wireless protocol standard. The 802.11n APs are backward-compatible with existing 802.11a/b/g networks and devices. The AP38xx and AP39xx series APs support the 802.11ac wireless protocol.

- The AP3705i delivers data rates up to 300 Mbps per radio; the AP37xx series APs except for the AP3705i deliver data rates up to 450 Mbps per radio.
- The AP38xx series APs deliver data rates up to 1.3 Gbps on Radio 1 (the 5 GHz radio) and 450 Mbps on Radio 2 (the 2.4 GHz radio)
- The AP39xx series supports an internal antenna array and active/active E/N data ports that deliver data rates up to 1.7 Gbps on Radio 1 and 600 Mbps on Radio 2.

To configure an 802.11n/ac AP to achieve this high link rate, see [Achieving High Throughput with 11n and 11ac Wireless APs](#) on page 187.

Antennas

Some wireless AP models have built-in, internal antennas; some support external antennas. APs with internal antennas are certified as a complete unit. External antennas are individually certified for maximum transmitting power and determination of available channels in each country in which the AP is deployed.

The latest AP3915i/e and AP3917i/e models offer both Wi-Fi antennas and IoT antennas that are used to receive iBeacon signals from IoT devices.

For a list of the external antennas that can be used with each AP model and how to install them, refer to the *Installation Guide* for each AP and to the [ExtremeWireless External Antenna Site Preparation and Installation Guide](#).

Wireless APs with external antenna ports must be configured to associate the external antenna connected to each antenna port. For more information, see [Configuring Wireless AP Properties](#) on page 156.

AP Types (Features)

AP model types are differentiated by their feature design, particularly:

- Indoor/Outdoor — APs are built for either indoor or outdoor service.
 - Indoor APs are built for use in enclosed, protected areas (like inside buildings) where they are not exposed to harsh weather or temperature extremes. Indoor APs have optional mounting brackets for mounting the AP on walls or drop ceilings.
 - Outdoor APs are built weather-hardened, with watertight fittings for cables and antennas, splash guards, and a greater resistance to temperature extremes (both cold and heat). Outdoor APs can

extend your Wireless LAN to outdoor locations without Ethernet cabling. Mounting brackets are available to enable quick and easy mounting of the Outdoor APs to walls, rails, and poles.

- **Controller-based** — Controller-based APs are intended to be controlled centrally by an ExtremeWireless Appliance. All AP and service configuration, bridging, and networking is done on the controller, with the AP acting as the remote access point relaying communications between the network (the controller) and end-user devices.
- **Cloud-enabled** — Cloud-enabled APs are intended to be controlled by ExtremeCloud™ an easy to use and scalable cloud-based management platform that supports and transforms with your business. Combined with enterprise-grade wired and wireless cloud-managed devices, ExtremeCloud delivers a scalable and highly available pay-as-you go subscription solution.
- **IoT ready, smoke detector models** — ExtremeWireless offers APs that are equipped with IoT antennas for receiving iBeacon signals from IoT devices. The controller collects and filters data based on configuration parameters, and forwards the data to an Application Server for reporting. The AP3915i/e and AP3917i/e are equipped with IoT antennas.

Additionally, the indoor model (AP3915i/e) is equipped with a smoke detector.

The AP3912 and AP3916 models are equipped with BLE radios that send iBeacon signals to IoT devices.

- **AP 3916ic (Integrated Camera)** — 2x2 11ac AP with an integral security camera (2MP camera with resolution up to 1080p) that lets you extend your Wireless LAN and provide simultaneous wireless service, BLE or 802.15.4 coverage and security in public spaces, such as classrooms and offices. This fully featured access point can be mounted on the ceiling or wall. The integral ONVIF compatible security camera is connected to an internal wired Ethernet port. The AP3916ic provides flow based data handling for the wireless and wired connections. Enabled for ExtremeCloud™ support.
- **AP 3912 Wall Plate** — 2x2 11ac AP that is installed replacing other existing Ethernet wall plates with one or two ports. One Ethernet port on the wall plate must be connected to the LAN1 uplink connection on the AP (black). This link provides AF or AT POE to the AP and uplink data connectivity to the network. The other Ethernet port on the wall plate can be connected to the pass-through port on the AP (blue), allowing connection options for wired devices like IP phones. The AP3912 is intended to take advantage existing wired Ethernet outlets and a switch port. The AP3912 is installed over an existing wall plate, and it is connected to the existing cable / switch port. The AP offers an integrated BTLE/802.15.4 radio for connectivity to Internet of Things (IoT) sensors and devices. Enabled for ExtremeCloud™ support.
- **Threat Detection and Prevention Capability** —As the potential for wireless security threats grows, APs must evolve to detect and counter hostile intrusion and attacks. The AP37xx, AP38xx, AP39xx and W78xC series of access points are designed to support Radar channel monitoring and are configurable for protection against detected attacks.

The Radar and Mitigator functions are described in greater detail in [Threat Detection and Prevention Features](#) on page 105. Configuration of these functions on controllers is described in [Working with ExtremeWireless Radar](#) on page 563.

Other differentiating features in an AP product series are the number of internal or external antennas (see [Antennas](#) on page 102) or the number of radios the AP has (see [Radios](#) on page 103).

Radios

All wireless APs are equipped with at least two radios — Radio 1 and Radio 2:

- Radio 1 supports a 5 GHz radio band
- Radio 2 supports a 2.4 GHz radio band

**Note**

The following APs offer integrated BLE/802.15.4 radios: AP3912i , AP3915i/e, AP3916ic, AP3917i/e/k.

The AP39xx supports up to 1.7 Gbps on the 5 GHz radio and 600 Mbps on the 2.4 GHz radio using four spatial streams.

The 38xx and AP37xx series radios (except AP3705i) support up to 450Mbps using three spatial streams.

The radios are enabled or disabled through the Wireless Assistant. For more information, see [Modifying 11n and 11ac Wireless AP Radio Properties](#) on page 178.

The Unlicensed National Information Infrastructure (U-NII) bands all lie within the 5 GHz band, designed for short-range, high-speed, wireless networking communication.

802.11n APs support the full range of frequencies available in the 5 GHz band:

- 5150 to 5250 MHz - U-NII Low band
- 5250 to 5350 MHz - U-NII Middle Band
- 5470 to 5700 MHz - U-NII Worldwide
- 5725 to 5825 MHz - U-NII High Band

**Note**

802.11n-compliant wireless APs can achieve link rates of up to 300 Mbps. You can configure the controller for this higher level link rate. For more information, see [Achieving High Throughput with 11n and 11ac Wireless APs](#) on page 187.

AP3916ic (Integrated Camera)

The AP3916ic is an 11ac Wave 2 AP with an integral security camera that lets you extend your Wireless LAN and provide simultaneous wireless service, BLE or 802.15.4 coverage and security in public spaces, such as classrooms and offices.

The AP3916 can be mounted on the ceiling, wall or in a junction/gang box. The integral ONVIF compatible security camera is connected to an internal wired Ethernet port, and the AP provides policy enforcement control for the wireless and wired connections.

The AP3916ic has the following specifications:

- Integrated 2MP camera with resolution up to 1080p, with manual view adjustment.
- Radios: Two concurrent Wi-Fi radios (2.4 GHz and 5 GHz) and one additional radio that can operate as Bluetooth or 802.15.4.
- Antennas: Four internal single band Wi-Fi antennas and one internal antenna for Bluetooth (BLE) or 802.15.4.
- LEDs: Six
- 802.3af compliant for full functionality. Optional AC adapter.

- Supports the 802.11ac and 802.11n wireless standards, with full backward compatibility with legacy 802.11abg.
- 10/100/1000 Mbps operation.
- Adjustable mounting bracket (included) for drop-ceiling T-bar rail.
- Optional mounts can be purchased separately for junction/gang box, indoor wall and solid ceiling installation.
- Enabled for ExtremeCloud™ support.

ExtremeWireless support for the AP3916ic:

- Camera is powered by the AP3916i PoE power supply:
- Camera port (CAM) can be assigned through policy to B@AP or B@AC virtual network service topologies. Default and specific assignment is supported. You can use policy definition and assignment to provide network segmentation for network access and camera (CAM) functions.
- The AP3916ic's camera function is identified as "EXTR2MP-CAM" device type. Filter the appliance client list to obtain a list of cameras under the appliance management.
- The controller provides factory reset and restart functions for the camera.

Related Links

[AP3916ic Integrated Camera Deployment](#) on page 226

[Upgrading the Camera Image Manually](#) on page 237

[AP3916ic-Camera Web User Interface](#) on page 227

Threat Detection and Prevention Features

ExtremeWireless Appliances and the wireless APs they manage, provide Wireless Intrusion Detection Services (WIDS) and Wireless Intrusion Prevention Services (WIPS) to detect, report, and protect against potential wireless network attacks and threats such as rogue APs, AP spoofing, honeypot APs, password cracking, man-in-the-middle, denial of service (DoS), and others. The latest generation of controllers and the APs (AP39xx, AP38xx, AP37xx and W78xC series) implement the Radar feature and its major functions:

- Scanning channels for threat identification
- Analyzing and detecting a wide range of wireless security threats
- Taking active countermeasures (if configured to do so) against identified threats
- Validating WLAN (Wireless Local Area Network) Service configuration to protect against security weakness
- Generating threat event reports and forwarding them to Extreme Management Center™

All APs can simultaneously perform channel bridging and scan (monitor) the channels they are bridging. These APs can also be configured (on their controller) to perform countermeasures against detected threats. Radar threat detection scanning of channels on the APs is configured on In-Service Scan Profiles.

You can configure APs to operate as full time Radar agents by adding them to a Guardian Scan Profile. When operating in this mode, they are referred to as "Guardians." Once assigned to the Guardian Scan Profile, the APs stop forwarding traffic on both radios and devote all of their resources to threat detection and countermeasures. Any AP added to a Guardian Scan Profile is done so in its entirety. Therefore, it is not possible to dedicate one radio to scanning, and the other to forwarding. Guardian AP

can scan on multiple channels, which you can configure from the **Scan Profile Detection Settings** user interface. The AP cannot scan or transmit on channels that are prohibited by the regulations of the countries in which it is deployed.

Related Links

[Guardian Scan Profile Detection Settings](#) on page 578

[Working with ExtremeWireless Radar](#) on page 563

802.11n- and 802.11ac-Compliant Access Point Features

All 802.11n-compatible APs have the following features:

MIMO

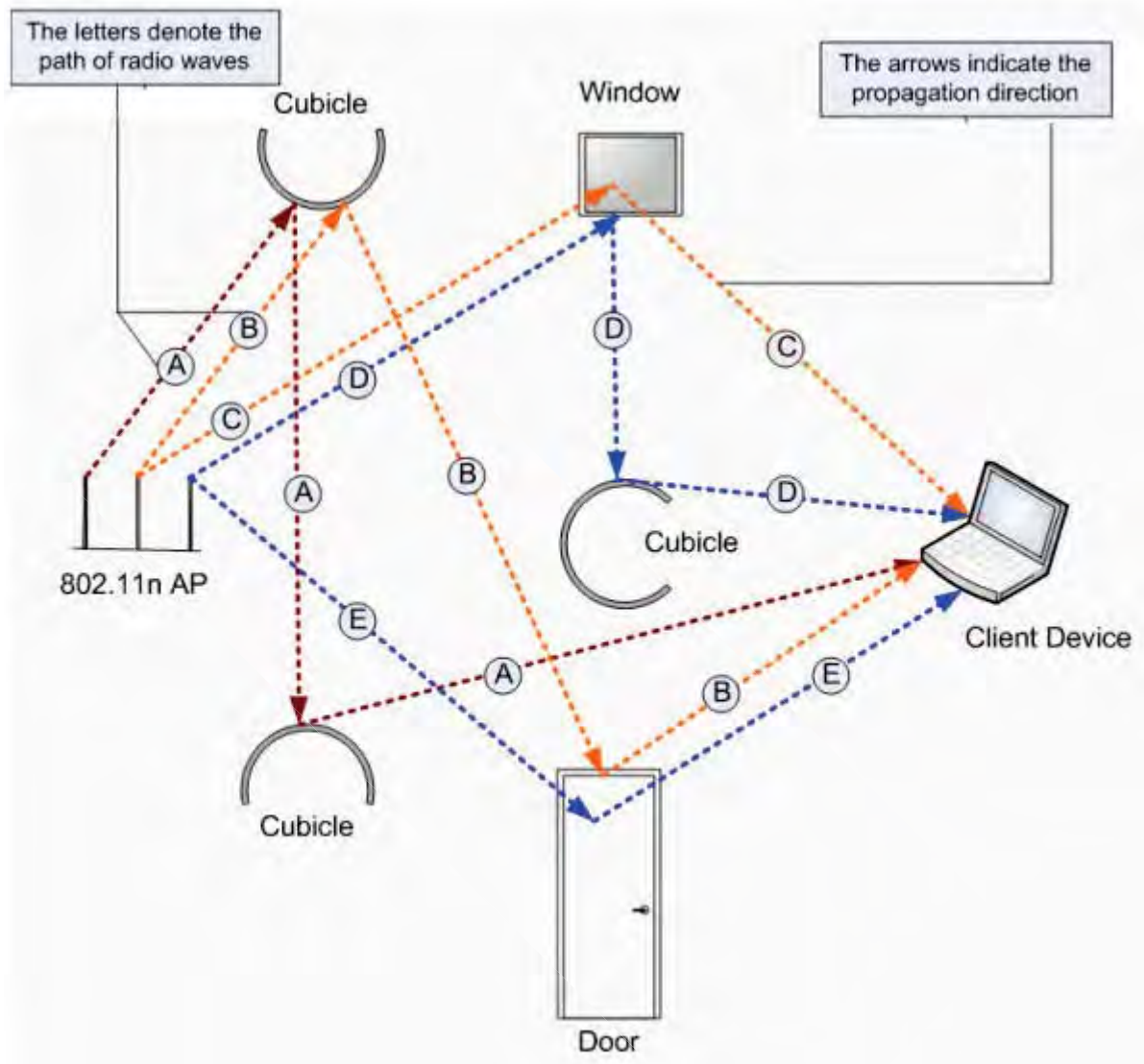
Wireless APs use MIMO (multiple input, multiple output) — a technology that uses advanced signal processing with multiple antennas to improve throughput. MIMO takes advantage of multipath propagation to decrease packet retries to improve the fidelity of the wireless network. MIMO increases throughput by using multiple streams.

MIMO radios send out one, two or three radio signals through each antenna. Each signal is called a spatial stream. The antennas on the AP are deliberately spaced so that each spatial stream follows a slightly different path to the client device. Two spatial streams get multiplied into several streams as they bounce off obstructions in the vicinity. This phenomenon is called multipath. As the streams are bounced from different surfaces, they follow different paths to the client device. The client device also has multiple antennas. Each of the antennas independently decodes the arriving signal. Then the decoded signal from each antenna combines with the decoded signals from the other antennas. A software algorithm uses this redundancy to extract one or two spatial streams and enhances the signal to noise ratio of the streams.

The client device also sends out one or two spatial streams through its multiple antennas. These spatial streams get multiplied into several streams as they bounce off the obstructions in the vicinity en route to the AP. MIMO receivers receive these multiple streams with three antennas. Each of the three antennas independently decodes the arriving signal. Then the decoded signal of each antenna is combined with the decoded signals from the other antennas. The receiving AP's MIMO receiver also uses redundancy to extract one or two spatial streams and enhances the streams' signal to noise ratio.

Operating with multiple antennas, an AP with MIMO is capable of picking up even the weakest signals from the client devices.

Figure 11: MIMO in Wireless APs



The AP39xx models offer Multi-User MIMO that enables Wave2 APs to communicate with multiple Wave2 clients concurrently, in the downstream direction. Up to 3 MU-MIMO conversations concurrently.

Channel Bonding

In addition to MIMO technology, the 802.11n-compliant APs have additional radio features that increase the effective throughput of the wireless LAN. Second-generation wireless APs use radio channels that are 20 MHz wide. The channels must be spaced at 20 MHz to avoid interference. The radios of 802.11n-compliant wireless APs can use two channels at the same time to create a 40-MHz-wide channel. The 802.11ac radio of the AP38xx and AP39xx series can use four channels at the same time to create an 80-MHz-wide channel. By using multiple 20-MHz channels in this manner, the wireless AP achieves more than double the throughput. The 40-MHz and 80-MHz channels in 802.11n and 802.11ac are adjacent 20-

MHz channels, bonded together. This technique of using multiple channels at the same time is called channel bonding.

Shortened Guard Interval

The purpose of the guard interval is to introduce immunity to propagation delays, echoes and reflections of symbols in orthogonal frequency division multiplexing (OFDM) — a method by which information is transmitted via a radio signal in APs.

In OFDM, the beginning of each symbol is preceded by a guard interval. As long as the echoes fall within this interval, they do not affect the safe decoding of the actual data, as data is interpreted only outside the guard interval. Longer guard periods reduce the channel efficiency. 802.11n-compliant APs provide reduced guard periods, thereby increasing the throughput.

MAC Enhancements

802.11n-compliant APs also have an improved MAC layer protocol that reduces overhead (in the MAC layer protocol) and contention losses, resulting in increased throughput.

Wireless AP International Licensing

A wireless AP must be configured to operate on the appropriate radio band in accordance with the regulations of the country in which it is being used. For more information, see [Regulatory Information](#) on page 705.

To configure the appropriate radio band according to the country of operation, use the controller. For more information, see [Configuring Wireless AP Properties](#) on page 156.

Related Links

[Licensing Considerations](#) on page 108

Licensing Considerations

With ExtremeWireless v10.01 and later each controller is licensed in a specific domain. The domain licenses include:

- FCC
- ROW
- MNT
- EGY

The user interface reflects the domain of the controller. The following are use cases for each domain:

- A wireless appliance with an FCC license can manage access points deployed in the United States, Puerto Rico, or Colombia.
- A wireless appliance with a ROW license can manage access points deployed in any country *except* the United States, Puerto Rico, Egypt, or Colombia.

- A wireless appliance with a EGY license will continue to require ROW hardware, but the license will restrict country selection to Egypt only. A wireless controller with a EGY license can manage access points deployed in Egypt.

**Note**

If upgrading from v10.21 with an EGY license, call customer support for assistance.

- A wireless appliance with a MNT license can manage only domain-locked access points, which are the AP39xx-FCC, AP39xx-ROW, and the AP3805i-FCC, AP3805i-ROW only. The FCC models must be deployed in the United States, Puerto Rico, or Colombia. The ROW must be deployed in any country *except* the United States, Puerto Rico, or Colombia.

**Note**

The AP37xx and AP38xx will NOT be able to connect to a controller licensed in the MNT domain.

First-time Configuration Guidelines

Wireless AP Default IP Address

Wireless APs are shipped from the factory with a default IP address — 192.168.1.20. The default IP address simplifies the first-time IP address configuration process for APs. If an AP fails in its discovery process, it returns to its default IP address. This AP behavior ensures that only one AP at a time can use the default IP address on a subnet. For more information, see [Discovery and Registration](#) on page 120.

Wireless APs can acquire their IP addresses by one of two methods:

- **DHCP assignment** — When an AP is powered on, it attempts to reach the *DHCP (Dynamic Host Configuration Protocol)* server on the network to acquire an IP address. If successful, the DHCP server assigns an IP address to the AP.
 - If the DHCP assignment is not successful in the first 60 seconds, the AP returns to its default IP address.
 - After 30 seconds in the default IP address mode, it attempts again to acquire an IP address from the DHCP server.
 - The process repeats until the DHCP assignment is successful, or until an administrator assigns the AP an IP address, using static configuration.

DHCP assignment is the default method for AP configuration. DHCP assignment is part of the discovery process. For more information, see [Discovery and Registration](#) on page 120.

- **Static configuration** —Use the static configuration option to assign a static IP address to a wireless AP. For more information, see the following section.

You can establish an SSH session with an AP during the time window of 30 seconds when the AP returns to its default IP address mode. If a static IP address is assigned during this period, reboot the AP for the configuration to take effect. For more information, see [Assigning a Static IP Address to a Wireless AP](#) on page 110.

Assigning a Static IP Address to a Wireless AP

Depending upon the network condition, you can assign a static IP address to a wireless AP using the Wireless Assistant (Controller's GUI). Refer to [Setting Up the Wireless AP Using Static Configuration](#) on page 199 for more information.

Configuring Wireless APs for the First Time

Before configuring an AP for the first time, confirm that the following tasks have already been performed:

- The ExtremeWireless Appliance has been installed and connected to the network. For more information, see [Configuring the ExtremeWireless Appliance](#) on page 31.
- The ExtremeWireless Appliance has been configured. For more information, see [Configuring the ExtremeWireless Appliance](#) on page 31.
- The wireless APs have been installed.

For installation information, refer to the respective AP Installation Guide.

Once the APs are installed, continue with the AP initial configuration:

- 1 Define parameters for the discovery process. For more information, see [Wireless AP Registration](#) on page 123.
- 2 Connect the AP to a power source to initiate the discovery and registration process. For installation information, refer to the respective AP Installation Guide.

General Configuration Methods

This section describes the methods you can use to modify the properties of APs in your network.

Modifying the Properties of Wireless APs Based on a Default AP Configuration

To reset the AP to the default configuration, select **AP Properties > Reset To Defaults**.

To configure a wireless AP with the system default AP settings:

- 1 From the top menu, click **AP** and select the AP to modify.
- 2 Click **Reset to Defaults** and click **OK** to confirm your changes.



Caution

If you reset an AP to defaults, its Search List is deleted, regardless of the settings in Common Configuration.

Modifying the Default Setting of Wireless APs Using the Copy to Defaults Feature

The **Copy to Defaults** feature allows the properties of an already configured AP to become the system's default AP settings.

To modify the system default AP settings based on an already configured AP:

- 1 From the main menu, click **AP** and select the AP whose properties you want to use as the default. You can modify the properties here if necessary.

- 2 Click **Copy to Defaults** and click **OK** to confirm your changes.

AP Multi-Edit Properties

When you use the **Multi-edit** function, only options that are explicitly modified are changed by the update. The APs shown in the **Wireless APs** list are supported by various versions of software. Only attributes that are common between software versions are available for multi-edit. Setting an attribute that does not apply to an AP does not cause an abort of the multi-edit operation.

Table 10: Multi-Edit AP Properties

Field	Description
AP Properties	
Location	<p>Define the location of the AP.</p> <p>When a client roams to an AP with a different location, Area Notification is triggered. The Area Notification feature is designed to track client locations within pre-defined areas using either the Location Engine (for more information, see Configuring the Location Engine on page 609) or the AP Location field. When the clients change areas, a notification is sent.</p> <p>Location functionality on the AP is useful when access to Extreme Management Center OneView is not available.</p>
Zone	<p>Zone allows the RADIUS client to send the AP Zone name as the BSSID instead of the radio MAC address. This feature can be enabled regardless of whether the Site is using centrally located or local RADIUS servers. Zone name is limited to 32 bytes. Each AP can have its own Zone label although it is often useful to assign the same Zone to multiple APs. It can be easier to base authorization decisions on the zone label rather than on the BSSID.</p>
Poll Timeout	<p>Type the timeout value, in seconds. The AP uses this value to trigger re-establishing the link with the Controller if the AP does not get an answer to its polling. The default value is 10 seconds.</p> <p>Note: If you are configuring session availability, the Poll Timeout value should be 1.5 to 2 times of Detect link failure value on AP Properties screen. For more information, see Session Availability on page 545.</p>

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Secure Tunnel	<p>This feature, when enabled, provides encryption, authentication, and key management between the AP and/or controllers.</p> <p>Select the desired Secure Tunnel mode from the drop-down list:</p> <ul style="list-style-type: none"> Disabled — Secure Tunnel is turned off and no traffic is encrypted. All SFTP/SSH/TFTP traffic works normally. Encrypt control traffic between AP & Controller — An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control traffic is encrypted. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. Encrypt control and data traffic between AP & Controller — This mode only benefits routed/bridged@Controller Topologies. An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control and data traffic is encrypted. The AP skips the registration and authentication phases, and when selected, the Secure Tunnel Lifetime feature can be configured. <p>Note: This option is not available for AP3805 models.</p> <ul style="list-style-type: none"> Debug mode — An IPSEC tunnel is established from the AP to the controller, no traffic is encrypted, and all SFTP/SSH/TFTP traffic works normally. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. <p>Note: Changing a Secure Tunnel mode will automatically disconnect and reconnect the AP.</p>
Secure Tunnel Lifetime (hours)	<p>Enter an interval (in hours) at which time the keys of the IPSEC tunnel are renegotiated.</p> <p>Note: Changing the Secure Tunnel Lifetime setting will not cause any AP disruption.</p>
Remote Access	Determines if the AP can be accessed remotely.
Location-based Service	<p>Enable or disable third-party location based services on this AP. ExtremeWireless supports the following third-party services:</p> <ul style="list-style-type: none"> AeroScout Ekahau Centrak
Maintain client session in event of poll failure	Determines if the AP remains active when a link loss with the controller occurs. Select this option when using a bridged at AP VNS. This option is enabled by default.
Restart service in the absence of controller	Determines if the AP's radios continue providing service when the AP's connection to the controller is lost. Select this option when using a bridged at AP VNS. When this option is enabled, the AP starts a bridged at AP VNS in the absence of a controller.

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Use broadcast for disassociation	Determines if the AP uses broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This setting affects the behavior of the AP when the AP is preparing to reboot or preparing to enter one of the special modes (DRM initial channel selection), and when a BSSID is deactivated or removed on the AP. This option is disabled by default.
LLDP	Determines if the AP broadcasts <i>LLDP (Link Layer Discovery Protocol)</i> information. This option is disabled by default. If <i>SNMP (Simple Network Management Protocol)</i> is enabled on the controller and you enable LLDP, the LLDP Confirmation dialog is displayed. Select one of the following: <ul style="list-style-type: none"> • Proceed (not recommended) — Select this option to enable LLDP and keep SNMP running. • Disable SNMP publishing, and proceed — Select this option to enable LLDP and disable SNMP. • For more information on enabling SNMP, see the <i>ExtremeWireless Maintenance Guide</i>.
Multicast prioritized as voice	Ensures that multicast data has the highest priority in the wireless network. Prioritizes multicast data to the level of voice data. This setting must be enabled when deploying healthcare patient monitoring devices.
IP Multicast Assembly	Determines if IP Multicast Assembly runs on the wireless AP. If enabled, IP Multicast Assembly joins together fragmented multicast data packets that are too large to fit the MTU size of the tunnel header. This feature is disabled by default.
Balanced Channel List Power	Simplify power settings so settings function across all channels in the channel plan.
LED	Select the desired LED pattern from the drop-down list. Options include: Off, WDS Signal Strength, Identify, and Normal.
Country	Indicates the country of operation. The antenna you select determines the available channel list and the maximum transmitting power for the country in which the AP is deployed.
Antennas	The Professional Install option is only available for AP models with external antennas. The fields and corresponding antenna value options that appear on the Professional Install dialog depend on the selected AP and the antenna models that are available. Select an antenna for each available port. By default, the two antennas must be identical. However, you have the option to select No Antenna for the second antenna port. The AP3915e and AP3917e access point models offer an external IoT antenna. Select the antenna model from the drop-down field. Choose the desired attenuation for each radio from the drop-down list. Selectable range is from 0 to 30 dBI.
Radio Settings	
Admin Mode	Determines if the radio mode. Select On to enable the radio. Select Off to disable the radio.

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Radio Mode	Select the radio mode based on the type of AP. Available radio settings are dependent on the selected radio mode.
Channel Width	Determines the channel width for the radio. Valid values are: <ul style="list-style-type: none"> 20 MHz — Allows 802.11n clients to use the primary channel (20 MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11b/g radio protocols. 40 MHz — Allows 802.11n clients that support the 40 MHz frequency to use 40 MHz, 20 MHz, or the 802.11b/g radio protocols. 802.11n clients that do not support the 40 MHz frequency can use 20 MHz or the 802.11b/g radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11b/g radio protocols. 80 MHz — Allows 802.11ac clients to use the 80 MHz frequency. Applies to AP38xx and AP39xx Radio 1 only. Auto — Automatically switches between 20 MHz, 40 MHz, and 80 MHz channel widths, depending on how busy the extension channels are.
DTIM	Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. Use a small number to minimize broadcast and multicast delay. The default value is 5.
Beacon Period	Defines the time, in milliseconds, between beacon transmissions. The default value is 100 milliseconds.
RTS/CTS (Bytes)	(Request to Send/Clear to Send) handshake. Determines the maximum packet size, in bytes, that triggers a RTS/CTS handshake. The default value is 2346 (the maximum 802.11 frame size) which means all packets are sent without RTS/CTS. If the transmitted packet size is greater than the threshold value, the RTS/CTS handshake occurs. Otherwise, the data frame is sent immediately. Reduce this value only if necessary. Note: In order for RTS/CTS to take affect, the RTS threshold must be less than or equal to the Frag threshold.
Frag Threshold (Bytes)	Determines the maximum packet size, in bytes, that triggers packet fragmentation. The default value is 2346. At 2346, all packets are sent unfragmented. Any value above the frag threshold triggers packet fragmentation by the AP prior to transmission.
RF Domain	Defines a group of APs that cooperate in managing RF channels and transmission power levels. The maximum string length is 16 characters.
Channel	Select Auto to use Automatic Channel Selection. For more information, see Dynamic Radio Management (DRM) on page 174.
Auto Tx Power Control	Determines if the AP automatically adapts transmission power signals according to the coverage provided by the AP. After a period of time, the system stabilizes itself based on the RF coverage of your wireless APs. When enabled, Min Tx Power and Auto Tx Power Ctrl Adjust parameters can be edited, and the ATPC algorithm adjusts the AP power between the Max Tx and Min Tx settings. When disabled, the radio uses the Max Tx Power value or the largest value in the compliance table, whichever is smaller.

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Max Tx Power	Determines the maximum power level used by the radio in dBm. The values are governed by compliance requirements based on the country, radio, and antenna selected, and vary by AP. Changing this value below the current Min Tx Power value will lower the Min Tx Power to a level lower than the selected Max TX Power. If Auto Tx Power Ctrl (ATPC) is disabled, the radio uses the selected value or the largest value in the compliance table as the power level, whichever is smaller.
Min Tx Power	Determines the minimum power level for the radio. Use the lowest supported value in order to not limit the potential Tx power level range that can be used. If ATPC is enabled, select the Min Tx power level that is equal or lower than the Max Tx power level. The Min Tx Power setting cannot be set higher than the Max Tx Power setting.
Auto Tx Ctrl Adjust	Determines if the AP automatically adapts transmission power signals according to the coverage provided by the AP. After a period of time, the system stabilizes itself based on the RF coverage of your wireless APs. When enabled, Min Tx Power and Auto Tx Power Ctrl Adjust parameters can be edited, and the ATPC algorithm adjusts the AP power between the Max Tx and Min Tx settings. When disabled, the radio uses the Max Tx Power value or the largest value in the compliance table, whichever is smaller.

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Channel Plan	<p>If ACS is enabled you can define a channel plan for the AP. Defining a channel plan allows you to control which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference.</p> <ul style="list-style-type: none"> • For 5 GHz Radio nodes, click one of the following: <ul style="list-style-type: none"> • All channels — ACS scans all channels for an operating channel and, when ACS is triggered, the optimal channel is selected from all available channels. • All Non-DFS Channels — ACS scans all non-DFS channels for an operating channel. With ACS, the AP selects the best non-DFS channel. • Custom — To configure individual channels from which the ACS selects an operating channel, click Configure. The Custom Channel Plan dialog displays. By default, all channels participate in the channel plan. Click the individual channels you want to include in the channel plan. To select contiguous channels, use the Shift key. To select multiple, non-contiguous channels in the list, use the CTRL key. Click OK to save the configuration. • All channels including weather radar — ACS selects the best channel from the available channels list. Selected channel may be DFS, weather-radar DFS or non-DFS. Weather-radar channels are approved for selected AP models in selected countries. Consult the compliance information for the selected AP. <p style="margin-left: 40px;">The weather channel includes 5600-5650MHz sub-bands and requires a listening period before the AP can provide wireless service. During the listening period, the Current Channel field for DFS channels displays the value <i>DFS Timeout</i>, and the weather channel fields display <i>DFS Timeout</i> . In Europe, the listening period can be up to 10 minutes. In the U.S., this period is 1 minute.</p> • For 2.4 GHz Radio nodes, click one of the following: <ul style="list-style-type: none"> • 3 Channel Plan — ACS scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in the rest of the world. • 4 Channel Plan — ACS scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world. • Auto — ACS scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world. • Custom — If you want to configure individual channels from which the ACS selects an operating channel, click Configure. The Add Channels dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click OK.

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Dynamic Channel Selection	Determines behavior when traffic or noise levels exceed the configured DCS thresholds. Valid values are: <ul style="list-style-type: none"> • Monitor Mode — An alarm is triggered and an information log is generated. • Active Mode — An alarm is triggered, an information log is generated, the AP stops operating on the current channel, and ACS automatically selects an alternate channel for the AP to operate on.
DCS Noise Threshold	Defines the noise interference limit, measured in dBm. If the noise interface exceeds this threshold, ACS scans for a new operating channel for the AP.
DCS Channel Occupancy Threshold	Defines the channel utilization level, measured as a percentage. If the threshold is exceeded, ACS scans for a new operating channel for the AP.
DCS Update Period (Minutes)	Defines a period of time, in minutes, where the average values for DCS Noise and Channel Occupancy are measured. If the average value for either setting exceeds the defined threshold for that setting, then the AP triggers Automatic Channel Scan (ACS).
Dynamic Channel Selection (DCS) events	Indicates items that can affect DCS (Dynamic Channel Selection). Enable one or more events if they are part of the wireless network: <ul style="list-style-type: none"> • Bluetooth • Microwave • Cordless Phone • Constant Wave • Video Bridge
Interference Wait Time	Length of the delay (in seconds) before logging an alarm. Default setting is 10 seconds.
Preamble	Select a preamble type for 11b-specific (CCK) rates: Short, or Long. Click Short if you are sure that there is no 11b APs or client in the vicinity of this AP. Click Long if compatibility with 11b clients is required.
Protection Mode	When data collides on a given channel, CTS (clear to send) protection determines which device transmits at a given time. <ul style="list-style-type: none"> • Auto. The default and recommended setting. • None. Select if 11b APs and clients are not expected. • Always. Select if you expect many 11b-only clients.
Protection Rate	A CTS (Clear to Send) packet is always sent out at the MBR (Minimum Basic Rate) configured for the radio. Protection is used when the sending rate (to the client) is greater than the configured protection rate. For example, if the protection rate is 11Mbps it means that 802.11 protection is used.

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Protection Type	Select a protection type: <ul style="list-style-type: none"> • CTS (Clear to Send) Only. • RTS (Request to Send) and CTS. Recommended when a 40 MHz or 80 MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
Min Basic Rate	Defines the minimum data rate that must be supported by all stations in a BSS (Base Station Subsystem): <ul style="list-style-type: none"> • Select 1, 2, 5.5, or 11 Mbps for 11b and 11b+11g modes. • Select 6, 12, or 24 Mbps for 11g-only mode. • Select 6, 12, or 24 Mbps for 11a mode.
Probe Suppression	Used to remedy "sticky clients", that is clients that do not probe on other channels and remain associated to an AP when a better AP is available. Configure per radio (Enable/Disable and Threshold). Applies to AP37xx, AP38xx, and AP39xx series APs. Probe Suppression accomplishes the following: <ul style="list-style-type: none"> • RSS threshold (Adjustable "Cell Size") • Reduces the number of Probe Responses. • Prevents clients with RSS below the threshold from associating.
Force Disassociate	Field is available when Probe Suppression is enabled. This setting does the following: <ul style="list-style-type: none"> • Disassociates "Sticky Clients" • Occurs 5dBm below the suppression threshold. • Prevents clients from re-associating to the AP. • Encourages/Forces roaming to a better AP. Configure per radio (Enable/Disable).
RSS Threshold (dBm)	90 (Range of -50 to -100). Field is available when Probe Suppression is enabled.
Max % of non-unicast traffic per Beacon period	Defines the maximum percentage of time that the AP transmits non-unicast packets (broadcast and multicast traffic) for each configured Beacon Period. For each non-unicast packet transmitted, the system calculates the airtime used by each packet and drops all packets that exceed the configured maximum percentage. Restrict non-unicast traffic, to limit the impact of broadcasts and multicasts on overall system performance.
Optimized Multicast for power save	Enables several performance enhancements applicable to clients in power save mode. One of these enhancements converts multicast to unicast for power save clients when the ratio of active to power save clients is sufficiently large.
Adaptable rate for Multicast	Determines if the AP tracks the lowest unicast transmission speed of any station currently associated to the AP. Multicast frames are then forwarded at that speed or at the Minimum Basic Rate, whichever is higher.

Table 10: Multi-Edit AP Properties (continued)

Field	Description
Multicast to Unicast delivery	<p>Determines if multicast packets are replaced by one unicast packet per destination station. Each unicast packet is transmitted at the highest speed the destination station will accept. Note: It is possible that some client devices will not handle frames properly when the L2 MAC is unicast and the L3 IP address is multicast in which case the "Multicast to Unicast Delivery" option should be disabled.</p> <p>Note: The AP converts a multicast frame to unicast frames only when it determines that it is more efficient to do so. With the exception of "Optimized Multicast for power save" these options can be enabled at any time without service disruption.</p>
11n Radio Settings	
Guard Interval	<p>Ensures that individual transmissions do not interfere with one another. It is the space between the symbols being transmitted. Selecting Short increases throughput, but can increase interference. Selecting Long can increase overhead due to additional idle time. The wireless 802.11n AP provides a shorter guard interval, which increases channel throughput. Long guard periods reduce channel efficiency.</p>
Protection Mode	<p>When data collides on a given channel, CTS (clear to send) protection determines which device transmits at a given time.</p> <ul style="list-style-type: none"> • Auto. The default and recommended setting. • None. Select if 11b APs and clients are not expected. • Always. Select if you expect many 11b-only clients.
Protection Type	<p>Select a protection type:</p> <ul style="list-style-type: none"> • CTS (Clear to Send) Only. • RTS (Request to Send) and CTS. Recommended when a 40 MHz or 80 MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
Extension Channel Busy Threshold	<p>CTS Only or RTS CTS, when a 40 MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.</p>
Aggregate MSDUs	<p>Determines MAC Service Data Unit (MSDU) aggregation. Enable to increase the maximum frame transmission size.</p>
Aggregate MPDUs	<p>Determines MAC Protocol Data Unit (MPDU) aggregation. Enable to increase the maximum frame transmission size, providing a significant improvement in throughput.</p>
Aggregate MPDU Max Length	<p>Defines the maximum length of the MAC Protocol Data Unit (MPDU) aggregation. Valid values range from 1024-65535 bytes. For the 802.11ac radio (Radio 1 of the AP38xx), the range is 1024-1048575.</p>
Agg. MPDU Max # of Sub-frames	<p>Determines the maximum number of sub frames in the aggregate MAC Protocol Data Unit (MPDU). Valid value range is 2-64. The default value and recommended value is 64. Setting this value to 64 results in less overhead and higher throughput.</p>

Table 10: Multi-Edit AP Properties (continued)

Field	Description
ADDBA Support	Block acknowledgement. Provides acknowledgement of a group of frames instead of a single frame. ADDBA Support must be enabled if Aggregate MPDU is enable.
LDPC	Increases the reliability of the transmission resulting in a 2dB increased performance compared to traditional 11n coding.
STBC	Space Time Block Coding. A simple open loop transmit diversity scheme. When enabled, STBC configuration is 2x1 (two spatial streams combined into one spatial stream). TXBF overrides STBC if both are enabled for single stream rates.
TXBF	Tx Beam Forming is a technique of re-aligning the transmitter multipath spatial streams phases in order to get better signal-to-noise ratio on the receiver side. For the AP37xx and AP38xx models, valid values are Enabled or Disabled. For the 39xx APs, this setting is only available on Radio1. The valid values are: MU_MIMO and Disabled.
Static Configuration	
EWC Search List	Defines the list of IP addresses that the AP is configured to try to connect to in the event that the current connection to the controller is lost.
Tunnel MTU	Maximum transmission unit. Determines the largest packet size than can be transmitted by an IP interface without the packet needing to be broken down into smaller units.
WLAN Assignments	
WLAN Assignment Option	Determines action on the WLAN assignment list associated with one or more APs. Valid values are Clear WLAN List or Reconfigure WLAN List .

Discovery and Registration

When a wireless AP is powered on, it automatically begins a discovery process to determine its own IP address and the IP address of the controller. When the discovery process is successful, the AP registers with the controller. For more information, see [Figure 12](#).



Warning

Only use power supplies that are recommended by Extreme Networks.

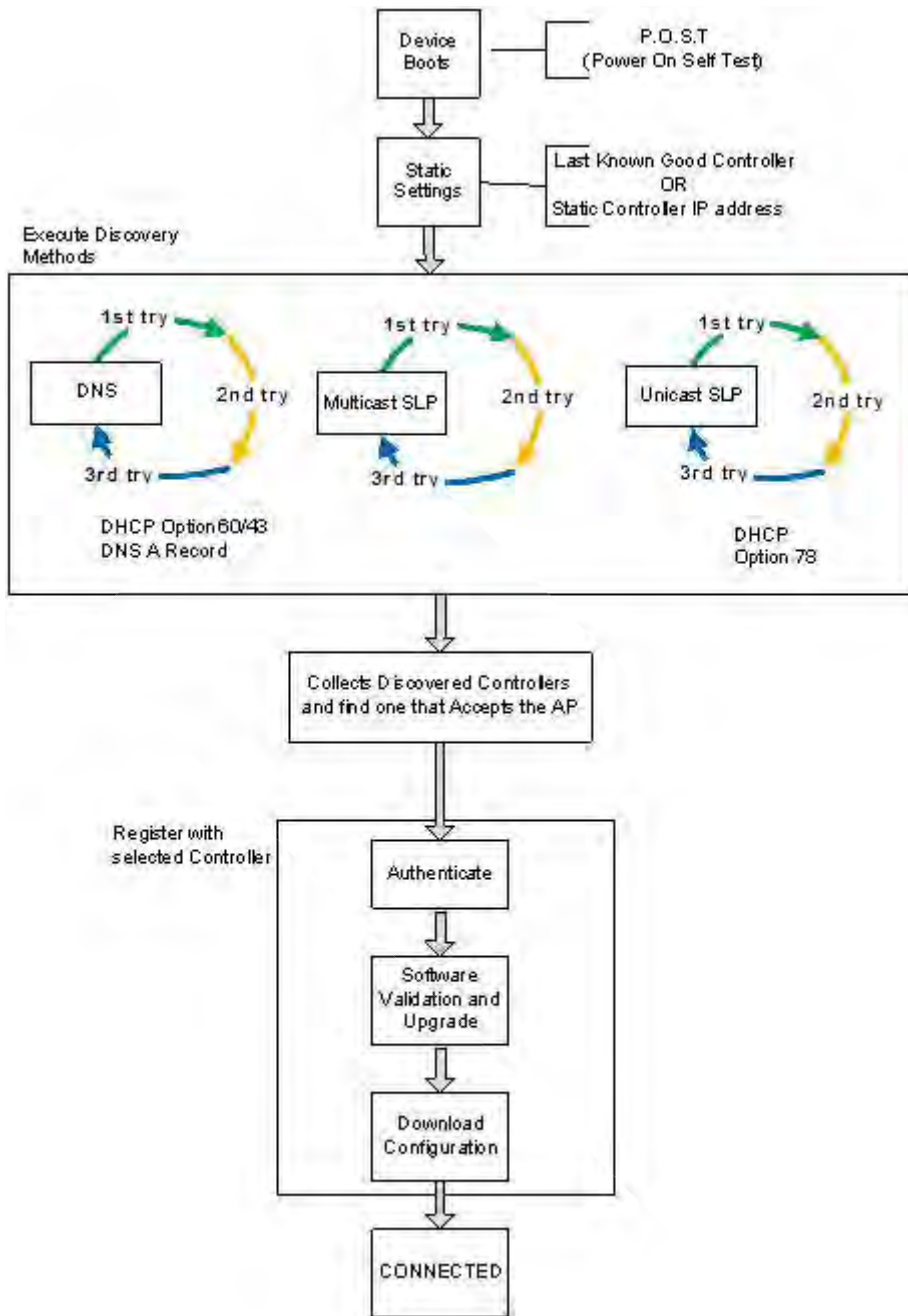


Figure 12: Wireless AP Discovery Process

Wireless AP Discovery

Wireless APs discover the IP address of a controller using a sequence of mechanisms that allow for the possible services available on the enterprise network. The discovery process is successful when the AP successfully locates a controller to which it can register.

Ensure that the appropriate services on your enterprise network are prepared to support the discovery process. The following steps are used to find a known controller:

- 1 Use the predefined static IP addresses for the controllers on the network (if configured).

You can specify a list of static IP addresses of the controllers on your network. On the **Static Configuration** tab, add the addresses to the **Wireless Controller Search List**.



Caution

Wireless APs configured with a static **Wireless Controller Search List** can connect only to controllers in the list. Improperly configured APs cannot connect to a non-existent controller address, and therefore cannot receive a corrected configuration.

- 2 Use the IP address of the controller to which the AP last connected successfully.

Once an AP has successfully registered with a controller, it recalls that controller's IP address, and uses that address on subsequent reboots. The AP bypasses discovery and goes straight to registration.

If a known controller cannot be located, the following discovery process steps should be followed:

- 3 Use **DHCP** Option 60 to query the DHCP server for available controllers. The DHCP server responds to the AP with Option 43, which lists the available controllers.

For the DHCP server to respond to an Option 60 request from an AP, configure the DHCP server with the vendor class identifier (VCI) for each AP. Also, configure the DHCP server with the IP addresses of the controllers. For more information, refer to the *Getting Started Guide*.

- 4 Use a Domain Name Server (DNS) lookup for the host name Controller.domain-name.

The AP tries the DNS server if it is configured in parallel with SLP unicast and SLP multicast.

If you use this method for discovery, place an A record in the DNS server for Controller.<domain-name>. The <domain-name> is optional, but if used, ensure it is listed with the DHCP server.

- 5 Use a multicast SLP request to find SLP SAs

The AP sends a multicast SLP request, looking for any SLP Service Agents providing the Extreme Networks service.

The AP tries SLP multicast in parallel with other discovery methods.

- 6 Use DHCP Option 78 to locate a Service Location Protocol (SLP) Directory Agent (DA), followed by a unicast SLP request to the Directory Agent.

To use the DHCP and unicast SLP discovery method, ensure that the DHCP server on your network supports Option 78 (DHCP for SLP RFC2610). The APs use this method to discover the controller.

This solution takes advantage of two services that are present on most networks:

- **DHCP** — The standard is a means of providing IP addresses dynamically to devices on a network.
- **SLP** — A means of allowing client applications to discover network services without knowing their location beforehand. Devices advertise their services using a Service Agent (SA). In larger installations, a Directory Agent (DA) collects information from SAs and creates a central repository (SLP RFC2608).

The controller contains an SLP SA that, when started, queries the DHCP server for Option 78 and if found, registers itself with the DA as service type Extreme Networks. The controller contains a DA (SLPD).

The AP queries DHCP servers for Option 78 to locate any DAs. The SLP User Agent for the AP then queries the DAs for a list of Extreme Networks SAs.

Option 78 must be set for the subnets connected to the ports of the controller and the subnets connected to the APs. These subnets must contain an identical list of DA IP addresses.

Wireless AP Registration

To define the discovery process parameters:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Registration**.

The following screen appears:

Wireless AP Registration

Security Mode:

Allow all Wireless APs to connect

Allow only approved Wireless APs to connect

Discovery Timers:

Number of retries: (1 - 255)

Delay between retries: (1 - 10 seconds)

SSH Access:

Password:

Confirm password:

Secure Cluster:

Cluster Shared Secret:

Use Cluster Encryption

- 3 Configure the following parameters:

Security Mode

- The **Allow all Wireless APs to connect** option is selected by default. For more information, see [Security Mode](#) on page 124.
- **Allow only approved Wireless APs to connect**

Discovery Timers . The discovery timer parameters dictate the number of retry attempts and the time delay between each attempt.

- **Number of retries**

- **Delay between retries**

The number of retries is limited to 255 for the discovery. The default number of retries is 3, and the default delay between retries is 3 seconds.

SSH Access

Set up a Secure Shell password. Click **Unmask** to display the password as you type.

- **Password**
- **Confirm Password**

Secure Cluster

Cluster Shared Secret. A common, default cluster ID.

- Click **Unmask** to display the shared secret value.
 - Check **Use Cluster Encryption**. If you disable cluster encryption, the AP cannot participate in the cluster.
- 4 Click **View SLP Registration** to confirm SLP Registration. A screen appears displaying the results of the diagnostic slpdump tool.
 - 5 From the Wireless AP Registration screen, click **Save** to save your changes.

Once the discovery parameters are defined, you can connect the AP to a power source. For instructions on connecting and powering an AP, refer to the *Installation Guide* for the specific AP.

Security Mode

Security mode defines how the controller behaves when registering new, unknown devices. During the registration process, the controller's approval of the AP's serial number depends on the security mode that has been set:

- **Allow all APs to connect**
 - If the controller does not recognize the registering serial number, a new registration record is automatically created for the AP (if within MDL license limit). The AP receives a default configuration. The default configuration can be the default template assignment.
 - If the controller recognizes the serial number, it indicates that the registering device is pre-registered with the controller. The controller uses the existing registration record to authenticate the AP and the existing configuration record to configure the AP.
- **Allow only approved APs to connect (this is also known as secure mode)**
 - If controller does not recognize the AP, the AP's registration record is created in pending state (if within MDL limits). The administrator is required to manually approve a pending AP for it to provide active service. The pending AP receives minimum configuration only, which allows it to maintain an active link with the controller for future state change. The AP's radios are not configured or enabled. Pending APs are not eligible for configuration operations (VNS Assignment, default template, Radio parameters) until approved.
 - If the controller recognizes the serial number, the controller uses the existing registration record to authenticate the AP. Following successful authentication, the AP is configured according to its stored configuration record.

During the initial setup of the network, Extreme Networks recommends that you select the **Allow all Wireless APs to connect** option. This option is the most efficient way to get a large number of APs registered with the controller. Once the initial setup is complete, Extreme Networks recommends that you reset the security mode to the **Allow only approved Wireless APs to connect** option. This option ensures that no unapproved APs are allowed to connect. For more information, see [Configuring Wireless AP Properties](#) on page 156.

Registration After Discovery

Any of the discovery steps 2 through 6 can inform the AP of a list of multiple IP addresses to which the AP may attempt to connect. Once the AP has discovered these addresses, it sends out connection requests to each of them. These requests are sent simultaneously. The AP attempts to register only with the first which responds to its request.

When the AP obtains the IP address of the controller, it connects and registers, sending its serial number identifier to the controller, and receiving from the controller a port IP address and binding key.

Once the AP is registered with a controller, configure the AP. After the AP is registered and configured, you can assign it to one or more Virtual Network Services (VNS) to handle wireless traffic.

The AP is registered with Secure mode and Un-secure mode. For new APs, that option is set in **AP Default Settings** dialog.

Viewing a List of All APs

To view a list of all APs:

- 1 From the top menu, click **AP**.

The screenshot shows the 'AP' tab in the configuration interface. At the top, there is a navigation bar with tabs for 'Logs', 'Reports', 'Controller', 'AP', 'VNS', and 'WIPS'. Below this is a search bar with the placeholder text 'Search for AP Name, Site, Model ...'. The main area contains a table with the following columns: Name, Model, Site, Location, SW Version, and Status. The table lists 10 APs with their respective details. Below the table, there is a summary line: 'Showing: 10 rows, Local: 5, Foreign: 5'. At the bottom, there are several action buttons: 'Actions', 'Radio 1 Actions', 'Radio 2 Actions', 'New', and 'Delete'.

<input type="checkbox"/>	Name ▲	Model ▾	Site ▾	Location ▾	SW Version ▾	Status ▾
<input type="checkbox"/>	14300167085D0000	AP3825e			10.41.02.0002T	Foreign
<input type="checkbox"/>	1548Y-1007900000	AP3965i-ROW	s1		10.41.01.0075T	Local
<input type="checkbox"/>	3916	AP3916ic-ROW			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3715i	AP3715i			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3765i	AP3765i			10.41.02.0002T	Local
<input type="checkbox"/>	AP3912i-ROW-1	AP3912i-ROW			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3915	AP3915e-ROW			10.41.02.0002T	Local
<input type="checkbox"/>	Dual band	AP3765e			10.41.02.0002T	Local
<input type="checkbox"/>	W786	W786C-2IA-RJ45			10.41.02.0002T	Foreign
<input type="checkbox"/>	W788	W788C-2-RJ45			10.41.02.0002T	Local

Showing: 10 rows, Local: 5, Foreign: 5

Actions Radio 1 Actions Radio 2 Actions New Delete

Search for any part of the AP string, any column of the AP list. Results:

- APs that match the search criteria appear.
- Select one or more APs and apply actions to selected APs.

- 2

At the top of the screen, enter search criteria and click .

APs that match the search criteria are displayed in the list.

- 3 To take action on one or more APs, select the check box for the AP and select an action from the **Actions** button. For more information, see [AP Actions](#) on page 128.
- 4 To view AP properties, click the AP row (not the check box). AP details are displayed.
- 5 Click **Configure** to display AP properties. For more information, see [AP Properties Tab Configuration](#) on page 159.
- 6 To add a new AP to the list, click **New > Create**. For more information, see [New Button -- Adding and Registering a Wireless AP](#) on page 131.
- 7 To add a new AP as a clone of an existing AP, click **New > Clone**. For more information, see [Creating a Clone AP](#) on page 133.

Related Links

[AP Search Facility](#) on page 127

[Understanding AP Status](#) on page 127

[AP Actions](#) on page 128

[Radio Actions](#) on page 130

[New Button -- Adding and Registering a Wireless AP](#) on page 131

[Deleting an AP](#) on page 134

[AP Properties Tab Configuration](#) on page 159

AP Search Facility

Search for any part of the AP string, any column of the AP list. Results:

- APs that match the search criteria appear.
- Select one or more APs and apply actions to selected APs.

To search, do the following:

1 Go to **AP > APs**.

2

At the top of the screen, enter search criteria and click .

APs that match the search criteria are displayed in the list.

Related Links

[AP Actions](#) on page 128

[Radio Actions](#) on page 130

[New Button -- Adding and Registering a Wireless AP](#) on page 131

[Deleting an AP](#) on page 134

[Understanding AP Status](#) on page 127

Understanding AP Status

The full AP list can be filtered to display just Foreign APs or just Local APs. When displaying a list of all APs, the value in the Status column is limited to Foreign or Local. In the left pane, click the **Foreign** or **Local** link to filter the list respectively. When the list is filtered, the value in the Status column changes.

Possible statuses for Local APs include:

- Pending. (You cannot view AP properties for Pending APs.)
- Active
- In-Active

Possible statuses for Foreign APs include:

- Active
- In-Active

For information about changing an AP's status, see [AP Actions](#) on page 128.

AP Actions

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

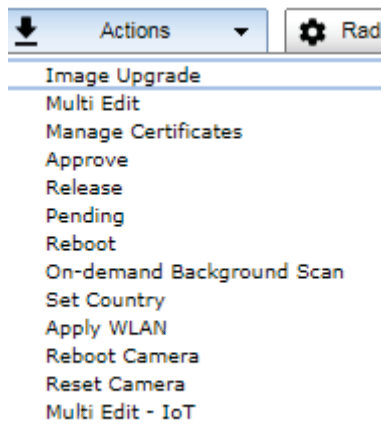


Figure 13: AP Actions button

Table 11: AP Actions

Field	Description
Image Upgrade	Select from the list of AP version images and apply to selected APs. If more than one AP is selected, the upgrade image must be common between the selected APs. If not, message displays indicating no common image. To upgrade without interrupting service, click Upgrade without interrupting service . If you click this option while the upgrade scheduler is running, the schedule is interrupted, and the current upgrade cycle calculates a new schedule that includes APs that weren't upgraded. Download appropriate image or select different APs. For information on downloading an upgrade image, see Downloading a new Wireless AP Software Image on page 240.
Multi Edit	Opens Multi Edit dialog for selected APs. Configuration changes are applied to selected APs only. For more information, see AP Multi-Edit Properties on page 111.
Manage Certificates	Opens Certificates screen for selected APs. Configuration changes are applied to selected APs only. For more information, see Managing Certificates on page 211
Approve	Approve — A Wireless AP's status changes from Pending to Approve if the AP Registration screen was configured to register only approved APs.
Release	Release foreign APs after recovery from a failover. Releasing an AP corresponds to the Availability function. For more information, see Availability and Session Availability on page 537.
Pending	Change Status to Pending — AP is removed from the Active list, and is forced into discovery.

Table 11: AP Actions (continued)

Field	Description
Reboot	Restart selected APs without using SSH to access it.
On-demand Background Scan	To verify channel assignments and review channel details without having to run a full ACS, run an on-demand background scan. For more information, see Running a Background Scan on page 638.
Set Country	Select from a list of countries and apply the command to the selected APs. You are prompted to confirm your selection.
Apply <i>WLAN</i>	The Apply WLAN dialog appears. Select the radio for each configured WLAN Service for the selected AP. List can contain 128 WLAN Services. You are prompted to confirm your selection. For AP3912 only, you can select the client port for each service. For the AP3916 only, you can select CAM on each service.
Reboot Camera	For AP3916 only. Restarts the camera on the AP.
Reset Camera	For AP3916 only. Resets the camera to factory default settings. After the camera is reset, a DHCP server is required to reassign IP addresses to the camera.
Multi Edit - IoT	Configure more than one AP for IoT support.

Related Links

- [IoT Multi-Edit Configuration](#) on page 129
- [IoT Thread Gateway](#) on page 196
- [Modifying the Status of a Wireless AP](#) on page 156
- [Assigning WLAN Services to Client Ports](#) on page 170

Applying WLAN Service

Select the radio for each configured WLAN Service for the selected AP. List can contain 128 WLAN Services. You are prompted to confirm your selection. For AP3912 only, you can select the client port for each service.

Related Links

- [Assigning WLAN Services to Client Ports](#) on page 170

IoT Multi-Edit Configuration

Configure more than one AP at a time for IoT support.

- 1 Select the check box next to more than one AP that supports the IoT.
The following APs offer integrated BLE/802.15.4 radios: AP3912i , AP3915i/e, AP3916ic, AP3917i/e/k.

- Click **Actions > Multi Edit - IoT**.

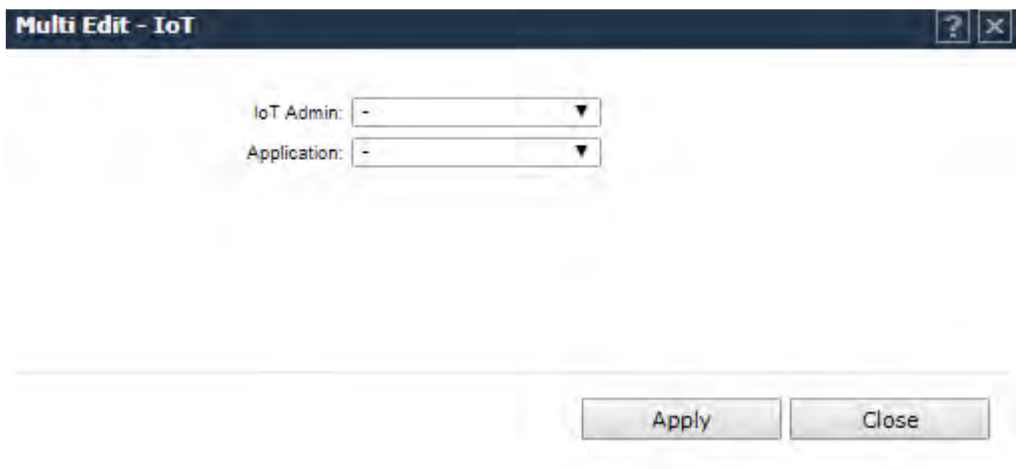


Figure 14: Multi-Edit - IoT Action

- Select **Enable** from the IoT Admin field.
- Select a value from the Application field. Valid values are **iBeacon**, **iBeacon Scan**, **Eddystone-url Beacon**, **Eddystone-url Scan**, or **Thread Gateway**. Resulting parameters depend on the application you select here.

Related Links

- [Configuring AP as an iBeacon on page 190](#)
- [Configuring iBeacon Scan on page 192](#)
- [Configuring AP as an Eddystone-url Beacon on page 194](#)
- [Configuring Eddystone-url Scan on page 195](#)
- [Advanced Thread Gateway Properties on page 198](#)

Radio Actions

Take the following actions from the Radio Actions button for the appropriate radio.

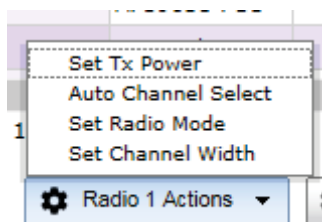


Figure 15: Radio 1 Actions

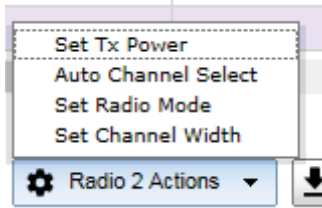


Figure 16: Radio 2 Actions button

Table 12: Radio Actions

Field	Description
Set Tx Power	Apply this command to selected APs. All selected APs must be the same model and licensed for the same country. Configure the setting from the resulting dialog. First, configure the selected APs to the same radio mode and same channel width before setting Tx Power here. When selected AP's are configured for the same width/mode, the Set Tx Power dialog displays the width/mode and you are able to set the Tx power and channel. For more information, see Configuration Parameters for Radio Properties on page 180.
Auto Channel Select	Apply this command to selected APs. For more information about ACS, see Dynamic Radio Management (DRM) on page 174.
Set Radio Mode	Apply this command to selected APs. All selected APs must be the same model and licensed for the same country. Configure the setting from the resulting dialog. For more information, see Configuration Parameters for Radio Properties on page 180.
Set Channel Width	Apply this command to selected APs. All selected APs must be the same model and licensed for the same country. Configure the setting from the resulting dialog. For more information, see Configuration Parameters for Radio Properties on page 180.

Related Links

[Configuration Parameters for Radio Properties](#) on page 180
[Dynamic Radio Management \(DRM\)](#) on page 174

New Button -- Adding and Registering a Wireless AP

You can manually add and register a wireless AP to the controller, but the AP must still go through the automatic discovery and registration process to locate the controller. The AP may skip the discovery process if it has a static list, or has previously connected and registered with the controller. When you manually add and register an AP, the system applies the default settings to the AP. After the system registers the AP, you can go in and edit its configuration settings (see [Configuring Wireless AP Properties](#) on page 156).

To add and register an AP manually:

- 1 From the top menu, click **AP**.

Regardless of the tab that you click on, the **New** button displays at the bottom of the page.

- 2 Click **New** and select **Create** or **Clone**.

Create Displays the **Add Wireless AP** dialog. For field descriptions, see [Table 13](#) on page 133.

Clone Displays the **Clone AP** dialog. See [Creating a Clone AP](#) on page 133.

The **Add Wireless AP** screen displays.

Add Wireless AP ? x

Serial #:

Hardware Type: Wireless AP3825i Internal ▼

Name:

Description:

Add Wireless AP

Wireless APs are added with default settings.
Individual Wireless AP settings may be modified via Wireless AP Configuration application.

Close

Table 13: Add Wireless AP

Field	Description
Serial #	Type the unique identifier of the AP.
Hardware Type	<p>Select the hardware model of this AP from the drop-down menu. With ExtremeWireless v10.01 each controller is licensed in a specific domain. There are three types of domain licenses: FCC, ROW, EGY, and MNT. The ExtremeWireless user interface reflects the domain of the controller. The following are use cases for each domain:</p> <ul style="list-style-type: none"> • A wireless controller with an FCC license can manage AP37xx, AP38xx, and AP39xx-FCC. These access points can be deployed in the United States, Puerto Rico, or Colombia. • A wireless controller with a ROW license can manage AP37xx, AP38xx, and AP39xx-ROW. These access points can be deployed in any country <i>except</i> the United States, Puerto Rico, Egypt, or Colombia. • A wireless controller with a MNT license can manage only domain-locked access points, which are the AP39xx-FCC and the AP39xx-ROW only. The AP39xx-FCC must be deployed in the United States, Puerto Rico, or Colombia. The AP39xx-ROW must be deployed in any country <i>except</i> the United States, Puerto Rico, Egypt, or Colombia. <p>Note: The AP37xx and AP38xx <i>cannot</i> connect to a controller licensed in the MNT domain.</p> <ul style="list-style-type: none"> • A wireless controller with a EGY license can manage AP37xx, AP38xx, and AP39xx-EGY.
Name	Type a unique name for the AP that identifies the access point. The default value is the AP's serial number.
Description	Enter a description of this AP.
Add Wireless AP	Click to add the AP with default settings. You can later modify these settings. When an AP is added manually, it is added to the controller database only and does not get assigned.
Close	Click to close this window.

Related Links

[Configuring Wireless AP Properties](#) on page 156

[Creating a Clone AP](#) on page 133

Creating a Clone AP

Create a new AP with the same type and configuration as the selected AP. Only one AP can be selected for the Clone action.

- 1 Select an AP from the AP list and click **New > Clone**.
- 2 Enter the **Serial #** and **Name** of the new clone AP.
- 3 Click **Apply**.

Related Links

[Viewing a List of All APs](#) on page 125

[New Button -- Adding and Registering a Wireless AP](#) on page 131

Deleting an AP

To delete an AP from the controller AP list:

- 1 Go to **AP > APs**.
- 2 Select the APs to delete.
- 3 Click **Delete**.

Wireless AP Default Configuration

Default wireless AP configuration acts as a configuration template that can be automatically assigned to new registering APs. The default AP configuration allows you to specify common sets of radio configuration parameters and VNS assignments for APs.

Configuring the Default Wireless AP Settings

Wireless APs are added with default settings. You can modify the system's AP default settings, and then use these default settings to configure newly added APs. In addition, you can base the AP default settings on an existing AP configuration or you can make pre-configured APs inherit the properties of the default AP configuration when they register with the system.

Each AP model has its own tab:

- **Common Configuration** — Configure common configuration, such as *WLAN* assignments and static configuration options for all APs. See [Configuring Common Configuration Default AP Settings](#) on page 135.
- **AP37xx W78xC**— Configure the default settings for the Radar series APs. See [Configuring AP37xx, W78xC Default AP Settings](#) on page 146.
- **AP37xx Dual Band** — Configure the default settings for the Radar series APs. See [Configuring AP37xx Dual Band Default Settings](#) on page 145
- **AP38xx**— Configure the default settings for the ExtremeWireless Radar series APs. See [Configuring AP38xx Default AP Settings](#) on page 143.
- **AP3801**— Configure the default settings for the ExtremeWireless Radar series APs. See [Configuring AP3801 Default AP Settings](#) on page 143.
- **AP3805**— Configure the default settings for the ExtremeWireless Radar series APs. See [Configuring AP3805 Default AP Settings](#) on page 144.
- **AP3912** — Configure the default settings for the ExtremeWireless wall plate AP. See [Configuring AP3912 Default AP Settings](#) on page 139.
- **AP3915** — Configure the default settings for the ExtremeWireless AP3915, BLE Radio enabled AP. See [Configuring AP3915 Default AP Settings](#) on page 138.
- **AP3916ic** — Configure the default settings for the ExtremeWireless Integrated Camera AP. See [Configuring AP3916 Default AP Settings](#) on page 137.
- **AP3917** — Configure the default settings for the ExtremeWireless AP3917, BLE Radio enabled AP. See [Configuring AP3917 Default AP Settings](#) on page 136.

- **AP3935** — Configure the default settings for the ExtremeWireless indoor series AP. See [Configuring AP3935 Default AP Settings](#) on page 140.
- **AP3965** — Configure the default settings for the ExtremeWireless outdoor series AP. See [Configuring AP3965 Default AP Settings](#) on page 142.

Configuring Common Configuration Default AP Settings

To configure common configuration default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.

The **Common Configuration** tab is displayed.

The screenshot shows the configuration interface for an AP. At the top, there is a navigation bar with tabs: Logs, Reports, Controller, AP (selected), VNS, WIPS. Below this is a sub-menu with tabs: Common Configuration (selected), AP3935 ROW, AP3965 ROW, AP376x W78xC, AP38xx, AP39xx. The main content area is divided into two sections: 'Static Configuration [Hide]' and 'WLAN Assignments [Hide]'. In the 'Static Configuration' section, there is a checkbox labeled 'Learn EWC Search List from AP' which is checked. In the 'WLAN Assignments' section, there is a checkbox labeled 'Apply default WLAN assignments to foreign APs' which is checked. Below this, there is a table for 'Associate radios:'.

WLAN Name	Airtime %	Radio 1	Radio 2	Ports
Lab46-WPA	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3

At the bottom right of the configuration area, there is a 'Save Settings' button.



Note

Ports 1, 2, and 3, are available on the AP3912. Port 1 is the port that corresponds to the Camera (CAM) function of the AP3916ic.

- 3 In the **Static Configuration** section, you can specify an EWC search list or use the search list provided from the AP. Do one of the following:
 - Check **Learn EWC Search List from AP** to accept the AP's search list, or clear the check box to specify a common search list for all APs. For more information about creating an EWC Search List, see [Table 22](#) on page 201.

- 4 In the **WLAN Assignments** section, you can associate a *WLAN* assignment to a radio.
 - If the controller is in an availability pair, you can apply default WLAN assignments to foreign APs, by selecting the **Apply default WLAN assignments to foreign APs** check box. For more information, see [Availability](#) on page 537.
 - To associate a WLAN Service in the list to a radio and or a client port, select the check box matching the radio and or port for the selected WLAN.
 - One WLAN can be assigned per port. The assignment enables the port.
 - Wireless and wired users associated to the same WLAN service receive identical service. They are affected by the same policies and filters.

**Note**

Airtime % is available for AP38xx and AP39xx access point models that are assigned WLANS configured with Reserved Airtime.

- 5 Click **Save Settings**.

Related Links

[Configuring Airtime Fairness: Reservation Mode](#) on page 406

Configuring AP3917 Default AP Settings

To configure AP3917 default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.

- Click the **AP3917 FCC** tab.

The screenshot shows the configuration interface for an AP3917 FCC. At the top, there is a navigation bar with tabs for AP3916 FCC, AP3916 ROW, AP37xx, AP3915 FCC, AP3915 ROW, and AP3917 FCC. The AP3917 FCC tab is highlighted with a red circle. Below the navigation bar, the 'AP Properties' section is expanded, showing the following settings:

- LLDP: Enabled
- Announcement Interval [Seconds]: 30
- Announcement Delay [Seconds]: 2
- Time To Live [Seconds]: 120
- Country: United States

Below the AP Properties section, the 'Radio Settings' section is expanded, showing settings for two radios:

	Radio 1	Radio 2
Admin Mode:	On	On
Radio Mode:	a/n/ac	b/g
Channel Width:	Auto	20MHz
RF Domain:	MyDomain	MyDomain
Auto Tx Power Ctrl:	Off	Off
Max Tx Power:	18 dBm	18 dBm
Min Tx Power:	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust:	0 dB	0 dB
Channel Plan:	All Non-DFS-Channel	Auto

Figure 17: AP3917 Default Settings

- Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- Click **Save Settings**.

Configuring AP3916 Default AP Settings

To configure AP3916 default AP settings:

- From the top menu, click **AP**.
- In the left pane, click **Global > Default Settings**.

- Click the **AP3916 ROW** tab.

The screenshot shows the configuration interface for an AP3916 ROW. At the top, a navigation bar contains tabs for various AP models: 7xx W78xC, AP38xx, AP3801, AP3805 ROW, AP3935 IL, AP3912 ROW, and **AP3916 ROW** (which is circled in red). Below the tabs, the 'AP Properties' section is expanded, showing settings for LLDP (Enabled), Announcement Interval (30 seconds), Announcement Delay (2 seconds), Time To Live (120 seconds), and Country (Austria). The 'Radio Settings' section is also expanded, displaying configurations for two radios. Radio 1 is set to Admin Mode: On, Radio Mode: a/n/ac, Channel Width: 40MHz, RF Domain: MyDomain, Auto Tx Power Ctrl: Off, Max Tx Power: 18 dBm, Min Tx Power: 0 dBm, Auto Tx Power Ctrl Adjust: 0 dB, and Channel Plan: All Non-DFS-Channel. Radio 2 is set to Admin Mode: On, Radio Mode: g/n, Channel Width: 20MHz, RF Domain: MyDomain, Auto Tx Power Ctrl: Off, Max Tx Power: 18 dBm, Min Tx Power: 8 dBm, Auto Tx Power Ctrl Adjust: 0 dB, and Channel Plan: Auto. At the bottom right, there are buttons for 'Advanced...' and 'Save Settings'.

Figure 18: AP3916 Default Settings

- Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- Click **Save Settings**.

Configuring AP3915 Default AP Settings

To configure AP3915 default AP settings:

- From the top menu, click **AP**.
- In the left pane, click **Global > Default Settings**.

- 3 Click the **AP3915 FCC** tab.

The screenshot shows the configuration interface for an AP3915 FCC. At the top, there is a navigation bar with tabs for AP3916 FCC, AP3916 ROW, AP37xx, **AP3915 FCC** (highlighted with a red circle), AP3915 ROW, and AP3917 FCC. Below the navigation bar, the 'AP Properties' section is expanded, showing the following settings:

- LLDP: Enabled
- Announcement Interval [Seconds]: 30
- Announcement Delay [Seconds]: 2
- Time To Live [Seconds]: 120
- Country: United States

Below the AP Properties section, the 'Radio Settings' section is also expanded, showing settings for two radios:

	Radio 1	Radio 2
Admin Mode:	On	On
Radio Mode:	a/n/ac	b/g
Channel Width:	Auto	20MHz
RF Domain:	MyDomain	MyDomain
Auto Tx Power Ctrl:	Off	Off
Max Tx Power:	18 dBm	18 dBm
Min Tx Power: ¹	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust:	0 dB	0 dB
Channel Plan:	All Non-DFS-Channel	Auto

Figure 19: AP3915 Default Settings

- 4 Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- 5 Click **Save Settings**.

Configuring AP3912 Default AP Settings

To configure AP3912 default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.

- Click the **AP3912 FCC** tab.

The screenshot shows the configuration interface for an AP3912 FCC. At the top, a navigation bar contains tabs for AP3965 FCC, AP37xx W78xC, AP38xx, AP3801, AP3805 FCC, and AP3912 FCC. The AP3912 FCC tab is highlighted with a red circle. Below the tabs, the 'AP Properties' section is expanded, showing settings for LLDP (Enabled), Announcement Interval (30 seconds), Announcement Delay (2 seconds), Time To Live (120 seconds), and Country (United States). The 'Radio Settings' section is also expanded, showing configurations for Radio 1 and Radio 2. Radio 1 settings include Admin Mode (On), Radio Mode (a/n/ac), Channel Width (40MHz), RF Domain (MyDomain), Auto Tx Power Ctrl (Off), Max Tx Power (18 dBm), Min Tx Power (0 dBm), Auto Tx Power Ctrl Adjust (0 dB), and Channel Plan (All Non-DFS-Channel). Radio 2 settings include Admin Mode (On), Radio Mode (g/n), Channel Width (20MHz), RF Domain (MyDomain), Auto Tx Power Ctrl (Off), Max Tx Power (18 dBm), Min Tx Power (8 dBm), Auto Tx Power Ctrl Adjust (0 dB), and Channel Plan (Auto). At the bottom right, there are buttons for 'Advanced...' and 'Save Settings'.

Figure 20: AP3912 Default Settings

- Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- Click **Save Settings**.

Configuring AP3935 Default AP Settings

ExtremeWireless 10.01 associates the license key to a specific Wireless Controller, and each license key applies to a specific regulatory domain (FCC or ROW). The FCC domain operates in the United States,

Colombia and Puerto Rico. The ROW domain operates outside these countries. The AP3935 can be licensed to operate within an FCC or ROW regulatory domain.

To configure AP3935 default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.
- 3 Click the **AP3935 FCC** tab.

The screenshot displays the configuration interface for the AP3935 FCC. The 'AP Properties' section is expanded, showing the following settings:

- LLDP: Enabled
- Announcement Interval [Seconds]: 30
- Announcement Delay [Seconds]: 2
- Time To Live [Seconds]: 120
- Country: United States

The 'Radio Settings' section is also expanded, showing settings for two radios:

	Radio 1	Radio 2
Admin Mode:	On	On
Radio Mode:	a/n/ac	b/g
Channel Width:	40MHz	20MHz
RF Domain:	MyDomain	MyDomain
Auto Tx Power Ctrl:	Off	Off
Max Tx Power:	18 dBm	18 dBm
Min Tx Power:	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust:	0 dB	0 dB
Channel Plan:	All Channels	Auto

Buttons for 'Advanced...', 'Save Settings', and 'Save Settings' are visible at the bottom of the configuration pane.

Figure 21: AP3935 FCC Default Settings

- 4 Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- 5 To save your changes, click **Save Settings**.

Configuring AP3965 Default AP Settings

ExtremeWireless 10.01 associates the license key to a specific Wireless Controller, and each license key applies to a specific regulatory domain (FCC or ROW). The FCC domain operates in the United States, Colombia and Puerto Rico. The ROW domain operates outside these countries. The AP3965 can be licensed to operate within an FCC or ROW regulatory domain.

To configure AP3965 default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.
- 3 Click the **AP3965 FCC** tab.

The screenshot displays the configuration interface for the AP3965 FCC. The top navigation bar shows several tabs: 'Common Configuration', 'AP3935 FCC', 'AP3965 FCC' (highlighted with a red circle), 'AP37xx W78xC', 'AP38xx', and 'AP3801'. Below the tabs, the 'AP Properties' section is visible, with a 'Hide' link. It contains the following settings:

- LLDP: Enabled
- Announcement Interval [Seconds]: 30
- Announcement Delay [Seconds]: 2
- Time To Live [Seconds]: 120
- Country: United States

The 'Radio Settings' section is also visible, with a 'Hide' link. It is organized into two columns: 'Radio 1' and 'Radio 2'. The settings for each radio are as follows:

Setting	Radio 1	Radio 2
Admin Mode	On	On
Radio Mode	a/n/ac	b/g/n
Channel Width	20MHz	20MHz
RF Domain	MyDomain	MyDomain
Auto Tx Power Ctrl	Off	Off
Max Tx Power	18 dBm	18 dBm
Min Tx Power	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust	0 dB	0 dB
Channel Plan	All Channels	Auto

At the bottom right of the configuration area, there are two buttons: 'Advanced...' and 'Save Settings'.

Figure 22: AP3965 FCC Default Settings

- 4 Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- To save your changes, click **Save Settings**.

Configuring AP38xx Default AP Settings

To configure AP38xx default AP settings:

- From the top menu, click **AP**.
- In the left pane, click **Global > Default Settings**.
- Click the **AP38xx** tab.

The screenshot shows the configuration interface for AP38xx. At the top, there are tabs for 'Common Configuration', 'AP3935 FCC', 'AP3965 FCC', 'AP37xx W78xC', and 'AP38xx' (which is circled in red). Below the tabs, there are sections for 'AP Properties' and 'Radio Settings'. The 'Radio Settings' section is divided into two columns: 'Radio 1' and 'Radio 2'. The settings for each radio are as follows:

Setting	Radio 1	Radio 2
Admin Mode:	On	On
Radio Mode:	a/n/ac	g/n
Channel Width:	20MHz	Auto
RF Domain:	MyDomain	MyDomain
Auto Tx Power Ctrl:	Off	Off
Max Tx Power:	18 dBm	18 dBm
Min Tx Power: ¹	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust:	0 dB	0 dB
Channel Plan:	All Non-DFS-Channel	Auto
Antenna Selection:	Left/Middle/Right	Left/Middle/Right

¹ Minimum power level is subject to the regulatory compliance requirement for the selected country

Figure 23: AP38xx Default Settings

- Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- To save your changes, click **Save Settings**.

Configuring AP3801 Default AP Settings

To configure AP3801 default AP settings:

- From the top menu, click **AP**.

- 2 In the left pane, click **Global > Default Settings**.
- 3 Click the **AP3801** tab.

The screenshot shows the configuration interface for an AP3801. At the top, there are tabs for 'Common Configuration', 'AP3935 FCC', 'AP3965 FCC', 'AP37xx W78xC', and 'AP3801'. The 'AP3801' tab is selected and circled in red. Below the tabs, there are two main sections: 'AP Properties' and 'Radio Settings', both with a '[Hide]' link. Under 'AP Properties', 'LLDP' is set to 'Disabled' and 'Country' is set to 'United States'. Under 'Radio Settings', there are two columns for 'Radio 1' and 'Radio 2'. The settings for Radio 1 are: Admin Mode: On, Radio Mode: a/n/ac, Channel Width: 40MHz, RF Domain: MyDomain, Auto Tx Power Ctrl: Off, Max Tx Power: 18 dBm, Min Tx Power: 0 dBm, Auto Tx Power Ctrl Adjust: 0 dB, and Channel Plan: All Non-DFS-Channel. The settings for Radio 2 are: Admin Mode: Off, Radio Mode: g/n, Channel Width: Auto, RF Domain: MyDomain, Auto Tx Power Ctrl: Off, Max Tx Power: 18 dBm, Min Tx Power: 8 dBm, Auto Tx Power Ctrl Adjust: 0 dB, and Channel Plan: Auto. At the bottom, there are two red footnotes: ¹ Minimum power level is subject to the regulatory compliance requirement for the selected country and ^{*} This setting may cause APs to reboot.

Figure 24: AP3801 Default Settings

- 4 Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- 5 To save your changes, click **Save Settings**.

Configuring AP3805 Default AP Settings

To configure AP3805 default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.

- Click the **AP3805 ROW** tab.

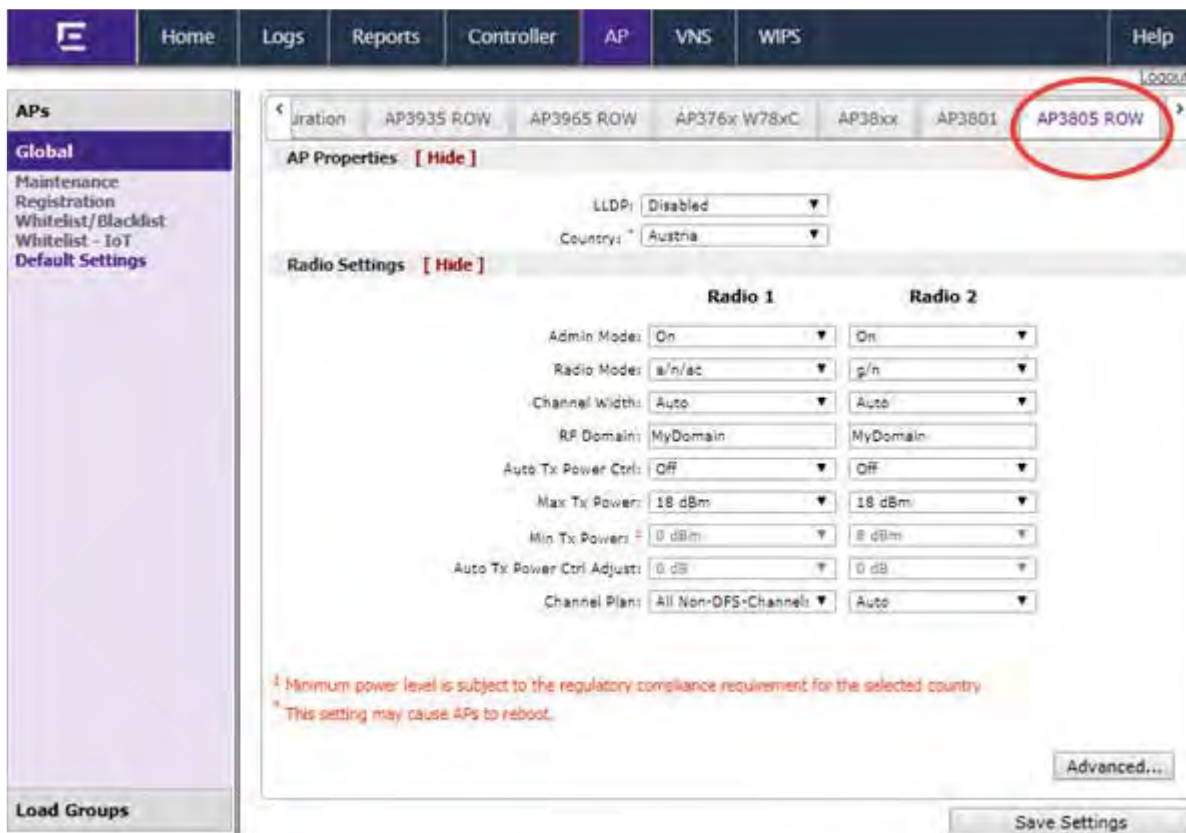


Figure 25: AP3805 Default Settings

- Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- To save your changes, click **Save Settings**.

Configuring AP37xx Dual Band Default Settings

This AP37xx profile supports two concurrent Wi-Fi radios (2.4 GHz and 5 GHz). To configure AP37xx default AP settings:

- From the top menu, click **AP**.
- In the left pane, click **Global > Default Settings**.

- 3 Click the **AP37xx** tab.

The screenshot shows the configuration interface for an AP37xx. At the top, a navigation bar contains tabs for different AP models: 805 ROW, AP3935 IL, AP3912 ROW, AP3916 ROW, **AP37xx** (highlighted with a red circle), AP3915 ROW, and AP. Below the navigation bar, the 'AP Properties' section is visible with 'LLDP' set to 'Disabled' and 'Country' set to 'Austria'. The 'Radio Settings' section is also visible, showing configurations for two radios. The settings for Radio 1 and Radio 2 are as follows:

	Radio 1	Radio 2
Admin Mode:	On	On
Radio Mode:	a	b/g
Channel Width:	20MHz	20MHz
RF Domain:	MyDomain	MyDomain
Auto Tx Power Ctrl:	Off	Off
Max Tx Power:	18 dBm	18 dBm
Min Tx Power:	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust:	0 dB	0 dB
Channel Plan:	All Non-DFS-Channel:	Auto
Antenna Selection:	Left/Middle/Right	Left/Middle/Right

Figure 26: AP37xx Default Settings

- 4 Configure the following Default AP Settings as required:
 - AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- 5 Click **Save Settings**.

Configuring AP37xx, W78xC Default AP Settings

To configure AP37xx, W78xC default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.

- 3 Click the **AP37xx W78xC** tab.

Common Configuration AP3935 FCC AP3965 FCC **AP37xx W78xC** AP38xx

AP Properties [Hide]

LLDP: Disabled ▾
Country: * United States ▾

Radio Settings [Hide]

	Radio 1	Radio 2
Admin Mode:	On ▾	On ▾
Radio Mode:	a/n ▾	g/n ▾
Channel Width:	Auto ▾	Auto ▾
RF Domain:	MyDomain	MyDomain
Auto Tx Power Ctrl:	Off ▾	Off ▾
Max Tx Power:	18 dBm ▾	18 dBm ▾
Min Tx Power: ¹	0 dBm ▾	8 dBm ▾
Auto Tx Power Ctrl Adjust:	0 dB ▾	0 dB ▾
Channel Plan:	All Non-DFS-Channel: ▾	Auto ▾
Antenna Selection: ⁴	Left/Middle/Right ▾	Left/Middle/Right ▾

¹ Minimum power level is subject to the regulatory compliance requirement for the selected country

Figure 27: AP37xx W78xC Default Settings

- 4 Configure the following Default AP Settings as required:
- AP Properties
 - Radio Settings
 - Advanced Settings

For detailed information, see [AP Default Settings](#) on page 148.

- 5 Click **Save Settings**.

AP Default Settings

Table 14: AP Default Settings

Field	Description
AP Properties	
LLDP	<p>Determines if the AP broadcasts <i>LLDP</i> information. This option is disabled by default.</p> <p>If <i>SNMP</i> is enabled on the controller and you enable LLDP, the LLDP Confirmation dialog is displayed.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> • Proceed (not recommended) — Enables LLDP and keeps SNMP (Simple Network Management Protocol) running. • Disable SNMP publishing, and proceed — Enables LLDP and disables SNMP. • For more information on using SNMP, see the Extreme Networks ExtremeWireless <i>Maintenance Guide</i>
Announcement Interval	<p>Determines how often the AP advertises its information by sending a new LLDP (Link Layer Discovery Protocol) packet when LLDP is enabled. This value is measured in seconds. If there are no changes to the AP configuration that impact the LLDP information, the AP sends a new LLDP packet according to this schedule.</p> <p>Note: Announcement Interval is not applicable on all AP models.</p>
Announcement Delay	<p>Determines the length of time that delays the new packet delivery. The announcement delay helps minimize LLDP (Link Layer Discovery Protocol) packet traffic when LLDP is enabled. This value is measured in seconds. If a change to the AP configuration occurs which impacts the LLDP information, the AP sends an updated LLDP packet.</p> <p>Note: Announcement Delay is not applicable on all AP models.</p>
Time to Live	<p>Determines the lifespan of the LLDP (Link Layer Discovery Protocol) packet. The Time to Live value is calculated as four times the Announcement Interval value. It cannot be directly edited.</p> <p>Note: Time to Live is not applicable on all AP models.</p>
Country	Select the country of operation.
Radio Settings (Radio 1 and Radio 2)	
Admin mode	Select On to enable this radio; Select Off to disable this radio.
Radio mode	<p>Click the radio mode based on the type of AP. For more information on the available Radio modes, see Configuring Wireless AP Radio Properties on page 174.</p> <p>The available radio settings are dependent on the radio mode you select.</p>

Table 14: AP Default Settings (continued)

Field	Description
Channel Width	<p>Click the channel width for the radio:</p> <ul style="list-style-type: none"> 20 MHz — Click to allow 802.11n clients to use the primary channel (20 MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11b/g radio protocols. 40 MHz — Click to allow 802.11n clients that support the 40 MHz frequency to use 40 MHz, 20 MHz, or the 802.11b/g radio protocols. 802.11n clients that do not support the 40 MHz frequency can use 20 MHz or the 802.11b/g radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11b/g radio protocols. 80 MHz — Click to allow 802.11ac clients to use the 80MHz frequency. Applies to AP38xx and AP39xx Radio 1 only. Auto — Click to automatically switch between 20 MHz, 40 MHz, and 80 MHz channel widths, depending on how busy the extension channels are.
RF Domain	<p>Uniquely defines a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 16 characters.</p>
Auto Tx Power Ctrl (ATPC)	<p>Determines if the AP will automatically adapt transmission power signals. Click to either enable or disable ATPC from the Auto Tx Power Ctrl drop-down list. ATPC automatically adapts transmission power signals according to the coverage provided by the AP. After a period of time, the system stabilizes itself based on the RF coverage of your Wireless APs.</p> <p>Note: When enabled, Min Tx Power and Auto Tx Power Ctrl Adjust parameters can be edited, and the ATPC algorithm will adjust the AP power between Max Tx power and Min Tx Power. When disabled, the Max Tx Power selected value or the largest value in the compliance table will be the power level used by the radio, whichever is smaller.</p>
Max Tx Power	<p>Click the appropriate Tx power level from the Max TX Power drop-down list. The values in the Max TX Power drop-down are in dBm and will vary by AP. The values are governed by compliance requirements based on the country, radio, and antenna selected. Changing this value below the current Min Tx Power value will change the Min Tx Power to a level lower than the selected Max TX Power.</p> <p>Note: If Auto Tx Power Ctrl (ATPC) is disabled, the selected value or the largest value in the compliance table will be the power level used by the radio, whichever is smaller.</p>
Min Tx Power	<p>If ATPC is enabled, select the minimum Tx power level that is equal or lower than the maximum Tx power level. We recommend that you use the lowest supported value if you do not want to limit the potential Tx power level range that can be used.</p> <p>Note: The Min Tx Power setting cannot be set higher than the Max Tx Power setting.</p>

Table 14: AP Default Settings (continued)

Field	Description
Auto Tx Power Ctrl Adjust	The Auto Tx Power Ctrl Adj parameter is a correction parameter that allows you to manually adjust (up or down) the Tx Power calculated by the ATPC algorithm. If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. Extreme Networks recommends that use 0 dB during your initial configuration. If you have an RF plan that recommends Tx power levels for each AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the Auto Tx Power Ctrl Adjust value to achieve the recommended values. Valid range is from $-(\text{Max Tx Power} - \text{Min Tx Power})$ dB to $(\text{Max Tx Power} - \text{Min Tx Power})$ dB.

Table 14: AP Default Settings (continued)

Field	Description
Channel Plan	<p>If ACS is enabled you can define a channel plan for the AP. Defining a channel plan allows you to control which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference.</p> <ul style="list-style-type: none"> • For 5 GHz Radio nodes, click one of the following: <ul style="list-style-type: none"> • All channels — ACS scans all channels for an operating channel and, when ACS is triggered, the optimal channel is selected from all available channels. • All Non-DFS Channels — ACS scans all non-DFS channels for an operating channel. With ACS, the AP selects the best non-DFS channel. • Custom — To configure individual channels from which the ACS selects an operating channel, click Configure. The Custom Channel Plan dialog displays. By default, all channels participate in the channel plan. Click the individual channels you want to include in the channel plan. To select contiguous channels, use the Shift key. To select multiple, non-contiguous channels in the list, use the CTRL key. Click OK to save the configuration. • All channels including weather radar — ACS selects the best channel from the available channels list. Selected channel may be DFS, weather-radar DFS or non-DFS. Weather-radar channels are approved for selected AP models in selected countries. Consult the compliance information for the selected AP. <p style="margin-left: 20px;">The weather channel includes 5600-5650MHz sub-bands and requires a listening period before the AP can provide wireless service. During the listening period, the Current Channel field for DFS channels displays the value <i>DFS Timeout</i>, and the weather channel fields display <i>DFS Timeout</i> . In Europe, the listening period can be up to 10 minutes. In the U.S., this period is 1 minute.</p> • For 2.4 GHz Radio nodes, click one of the following: <ul style="list-style-type: none"> • 3 Channel Plan — ACS scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in the rest of the world. • 4 Channel Plan — ACS scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world. • Auto — ACS scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world. • Custom — If you want to configure individual channels from which the ACS selects an operating channel, click Configure. The Add Channels dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click OK.

Table 14: AP Default Settings (continued)

Field	Description
Antenna Selection	<p>Antenna Selection — Click the antenna, or antenna combination, you want to configure on this radio.</p> <p>When you configure 11n Wireless APs to use specific antennas, the transmission power is recalculated; the Current Tx Power Level value for the radio is automatically adjusted to reflect the recent antenna configuration. It takes approximately 30 seconds for the change to the Current Tx Power Level value to be reflected in the ExtremeWireless Assistant. Also, the radio is reset causing client connections on this radio to be lost.</p> <p>Note: Antenna Selection is not applicable on all AP models.</p>
Advanced dialog – AP Properties	
Poll Timeout	<p>Type the timeout value, in seconds. The AP uses this value to trigger re-establishing the link with the controller if the AP does not get an answer to its polling. The default value is 10 seconds.</p> <p>Note: If you are configuring session availability, the Poll Timeout value should be 1.5 to 2 times of Detect link failure value on AP Properties screen. For more information, see Session Availability on page 545.</p>
Secure Tunnel	<p>This feature, when enabled, provides encryption, authentication, and key management between the AP and/or controllers.</p> <p>Select the desired Secure Tunnel mode from the drop-down list:</p> <ul style="list-style-type: none"> Disabled — Secure Tunnel is turned off and no traffic is encrypted. All SFTP/SSH/TFTP traffic works normally. Encrypt control traffic between AP & Controller — An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control traffic is encrypted. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. Encrypt control and data traffic between AP & Controller — This mode only benefits routed/bridged@Controller Topologies. An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control and data traffic is encrypted. The AP skips the registration and authentication phases, and when selected, the Secure Tunnel Lifetime feature can be configured. <p>Note: This option is not available for AP3805 models.</p> <ul style="list-style-type: none"> Debug mode — An IPSEC tunnel is established from the AP to the controller, no traffic is encrypted, and all SFTP/SSH/TFTP traffic works normally. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. <p>Note: Changing a Secure Tunnel mode will automatically disconnect and reconnect the AP.</p>

Table 14: AP Default Settings (continued)

Field	Description
Secure Tunnel Lifetime	Enter an interval (in hours) at which time the keys of the IPSEC tunnel are renegotiated. Note: Changing the Secure Tunnel Lifetime setting will not cause any AP disruption.
Remote Access	Click to Enable or Disable SSH to the AP.
Location-based Service	Click to Enable or Disable location-based service on this AP. Location-based service allows you to use this AP with an AeroScout or Ekahau solution.
Maintain client sessions in event of poll failure	Click to Enable or Disable (using a bridged at AP VNS) the AP remains active if a link loss with the controller occurs. This option is disabled by default.
Restart service in the absence of controller	Click to Enable or Disable (if using a bridged at AP VNS) to ensure the AP continues providing service if the AP's connection to the controller is lost. If this option is enabled, it allows the AP to start a bridged at AP VNS even in the absence of a controller.
Use broadcast for disassociation	Click to Enable or Disable if you want the AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This affects the behavior of the AP under the following conditions: <ul style="list-style-type: none"> • If the AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection). • If a BSSID is deactivated or removed on the AP. This option is disabled by default.
IP Multicast Assembly	Click to Enable or Disable multicast frames assembling for groups of APs using AP Multi-editing settings (for more information, see AP Multi-Edit Properties on page 111).
Balanced Channel List Power:	This simplifies power settings such that they will function across all channels in the channel plan.
LED	Select the desired LED pattern from the drop-down list. Options include: Off, WDS Signal Strength, Identify, and Normal.
Radio Settings	
DTIM	Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. Use a small number to minimize broadcast and multicast delay. The default value is 5.
Beacon Period	Defines the time, in milliseconds, between beacon transmissions. The default value is 100 milliseconds.
RST/CTS	Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is 2346, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
Frag. Threshold	Type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is 2346, which means all packets are sent un-fragmented.

Table 14: AP Default Settings (continued)

Field	Description
Dynamic Channel Selection	Click one of the following: <ul style="list-style-type: none"> • Monitor Mode – If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. • Active Mode – If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the AP ceases operating on the current channel and ACS automatically selects an alternate channel for the AP to operate on.
DCS Noise Threshold	Type the noise interference level, measured in dBm, after which ACS scans for a new operating channel for the AP if the threshold is exceeded.
DCS Channel Occupancy Threshold	Type the channel utilization level, measured as a percentage, after which ACS scans for a new operating channel for the AP if the threshold is exceeded.
DCS Update Period	Type the time, measured in minutes that determines the period during which the AP averages the DCS Noise Threshold and DCS Channel Occupancy Threshold measurements. If either one of these thresholds is exceeded, then the AP triggers ACS.
DCS Interference Event (appears if Dynamic Channel Selection is enabled)	Enable or disable the following DCS Events: <ul style="list-style-type: none"> • Bluetooth • Microwave • Cordless Phone • Constant Wave • Video Bridge
Interference Wait Time	Length of the delay (in seconds) before logging an alarm. Default setting is 10 seconds.
Preamble	Click a preamble type for 11b-specific (CCK) rates: Short, or Long. Click Short if you are sure that there is no 11b APs or client in the vicinity of this AP. Click Long if compatibility with 11b clients is required.
Protection Rate	Click a protection rate: 1, 2, 5.5, or 11 Mbps. The default and recommended setting is 11. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than 11 Mbps are required to ensure coverage.
Protection Mode	Click a protection mode: None, Auto, or Always. The default and recommended setting is Auto. Click None if 11b APs and clients are not expected. Click Always if you expect many 11b-only clients.
Protection Type	Click a protection type, CTS Only or RTS CTS, when a 40 MHz or 80 MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.

Table 14: AP Default Settings (continued)

Field	Description
Max % of non-unicast traffic per Beacon period	Enter the maximum percentage of time that the AP transmits non-unicast packets (broadcast and multicast traffic) for each configured Beacon Period. For each non-unicast packet transmitted, the system calculates the airtime used by each packet and drops all packets that exceed the configured maximum percentage. By restricting non-unicast traffic, you limit the impact of broadcasts and multicasts on overall system performance.
Optimized Multicast for power save	Click to optimize for power save.
Adaptable rate for Multicast	Click to enable adaptable rate capabilities.
Multicast to Unicast delivery	Click to set the Multicast to Unicast delivery method from the drop-down list.
Enhanced Rate Control	
Min. Basic Rate	For each radio, click the minimum data rate that must be supported by all stations in a BSS: <ul style="list-style-type: none"> Click 1, 2, 5.5, or 11 Mbps for 11b and 11b+11g modes. Click 6, 12, or 24 Mbps for 11g-only mode. Click 6, 12, or 24 Mbps for 11a mode.
11n Settings	
Protection Mode	Click a protection mode: None, Auto, or Always. The default and recommended setting is Auto. Click None if 11b APs and clients are not expected. Click Always if you expect many 11b-only clients.
Protection Type	Click a protection type, CTS Only or RTS CTS, when a 40 MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
Extension Channel Busy Threshold	Type the extension channel threshold percentage, which if exceeded, disables transmissions on the extension channel (40 MHz).
Aggregate MSDUs	Click an aggregate MSDU mode: Enabled or Disabled. Aggregate MSDU increases the maximum frame transmission size.
Aggregate MPDUs	Click an aggregate MPDU mode: Enabled or Disabled. Aggregate MPDU provides a significant improvement in throughput.
Aggregate MPDU Max Length	Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes.
Agg. MPDU Max # of Sub-frames	Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
ADDBA Support	Click an ADDBA support mode: Enabled or Disabled. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. ADDBA Support must be enabled if Aggregate MPDU is enable.
LDPC	Click an LDPC mode: Enabled or Disabled. LDPC increases the reliability of the transmission resulting in a 2dB increased performance compared to traditional 11n coding.

Table 14: AP Default Settings (continued)

Field	Description
STBC	Click an STBC mode: Enabled or Disabled. STBC is a simple open loop transmit diversity scheme. When enabled, STBC configuration is 2x1 (two spatial streams combine into one spatial stream). TXBF will override STBC if both are enabled for single stream rates.
TxBF	Tx Beam Forming is a technique of re-aligning the transmitter multipath spatial streams phases in order to get better signal-to-noise ratio on the receiver side. Click a TXBF mode: For the AP37xx and AP38xx models, valid values are Enabled or Disabled. For the 39xx APs, this setting is only available on Radio1 and valid values are MU-MIMO and Disabled.

Configuring Wireless AP Properties

Wireless APs are added with default settings, which you can adjust and configure according to your network requirements. In addition, you can modify the properties and the settings for each radio on the AP.

You can also locate and select APs in specific registration states to modify their settings. For example, this feature is useful when approving pending APs when there are a large number of other APs that are already registered. On the **Access Approval** screen, click **Pending** to select all pending APs, then click **Approve** to approve all selected APs.

Configuring AP settings can include the following processes:

- [Modifying the Status of a Wireless AP](#) on page 156
- [AP Properties Tab Configuration](#) on page 159
- [Setting Up the Wireless AP Using Static Configuration](#) on page 199

When configuring APs, you can choose to configure individual APs or simultaneously configure a group of APs. For more information, see [AP Multi-Edit Properties](#) on page 111.

Modifying the Status of a Wireless AP

If during the discovery process, the controller security mode was Allow only approved Wireless APs to connect, then the status of the AP is Pending. Modify the security mode to Allow all Wireless APs to connect.

Related Links

[Security Mode](#) on page 124

[AP Rehomng](#) on page 156

[AP Actions](#) on page 128

AP Rehomng

You can balance your AP deployment by switching an AP from local to foreign (and from foreign to local). The AP will continue providing service without interruption while the APs are redeployed. If the availability link is down, the conversion will be completed when the link is established.

The rehomed AP will establish an active tunnel to the new controller and radio configuration is preserved once conversion is complete.

- WLAN assignments are not affected by rehomings.
- WDS and Mesh APs cannot be converted from local to foreign.
- A rehomed AP will be removed from load balance groups.

AP Dashboard

ExtremeWireless offers a dashboard of statistical information for each AP in the network. The following information is displayed for each AP:

- IP address. Supports both IPv4 and IPv6 addresses.
- IoT MAC. Mac address for the Internet of Things enablement. Displays for AP3912 and AP3916 when IoT is enabled.
- Model Number
- Software version running on the AP
- Country
- AP Role
- Number of 802.3 clients (AP3912)
- Camera IP (AP3916)
- Number of radios
- Channel number if applicable
- Channel Mode
- Power level

The following APs offer integrated BLE/802.15.4 radios: AP3912i , AP3915i/e, AP3916ic, AP3917i/e/k.

AP properties for these access points display the IoT MAC address and channel and the TX Power Level for the BLE radio when the IoT is enabled.

The screenshot shows the AP3916ic dashboard. On the left, a list of properties includes IP (0.0.0.0), IoT MAC (00:00:00:00:00:01), Model (AP3916ic-FCC), Software Version (10.31.01.0044), Country (United States), Role (Traffic forwarder (AP)), and Camera IP. On the right, a table shows radio configuration for two radios. Radio 2 is highlighted with a green box, showing it is an IoT radio with a channel of '-' and a power level of 0 dBm.

IP	0.0.0.0	Radio	Channel	Mode	Power
IoT MAC	00:00:00:00:00:01	1			
Model	AP3916ic-FCC	2			
Software Version	10.31.01.0044	IoT	-	BLE	0 dBm
Country	United States				
Role	Traffic forwarder (AP)				
Camera IP					

Figure 28: AP3916 Dashboard with IoT Enabled

The dashboard displays a graphical representation over the last hour for the following:

- Client count. Associated clients per radio
- Devices by Type classification
- Noise floor for both bands
- Channel utilization for both bands



Figure 29: AP Dashboard

Clients

Displays the number of clients on each radio in 10-minute intervals. Use this information to gain visibility over time into AP utilization per radio. Details for the AP3912 and AP3916 show the number of 802.3 clients. These are clients that utilize the wired client ports that are available on these AP models.

Devices by Type

Offers visibility into the type of devices connected to your network by percentage. Use this information to understand the BYOD usage on your network.

Noise (dBm)

Tracks the noise level for each AP radio in 10-minute intervals. Use this information to understand channel performance over time.

Channel Utilization (%)

Tracks the percentage of traffic on each radio. Use this information to understand channel usage over time, in 10-minute intervals.

Click **Configure** to display configuration options for the AP. For more information, see [AP Properties Tab Configuration](#) on page 159.

Related Links

[AP Properties Tab Configuration](#) on page 159

[Channel Inspector Report](#) on page 637

AP Properties Tab Configuration

Use the **AP Properties** tab to view and configure basic AP properties. Some of the AP properties can be viewed and configured via the **Advanced** dialog.

- 1 From the top menu, click **AP**.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
For more information, see [AP Dashboard](#) on page 157.

- 3 Click **Configure**. The AP Properties tab displays.

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.1x
Serial #:	14160242085A0000				
Host Name:	AP3825e-14160242085A0000				
Name:	C5110 - ap3 - AP3825e				
Location:	MU7 - C5110				▶
Zone:					▶
Description:	<div style="border: 1px solid #ccc; height: 40px;"></div>				
Topology:	esa0				
AP Environment¹:	Indoor ▼				
	¹ Change of Environment will cause interruption of service				
Hardware Type:	Wireless AP3825e External				
Application Version:	10.11.01.0196				
Status:	Approved				
Active Clients:	0				
Role:	Traffic forwarder (AP)				
Country²:	United States ▼				
	² Change of Country may cause AP to reboot.				
				Professional install	Advanced...

Related Links

- [AP Dashboard](#) on page 157
- [AP Properties Tab - Basic Settings](#) on page 161
- [AP Properties Tab - Advanced Settings](#) on page 164
- [Professional Install Settings](#) on page 166
- [Assigning Wireless AP Radios to a VNS](#) on page 168
- [Configuration Parameters for Radio Properties](#) on page 180
- [Configuring IoT Applications](#) on page 189
- [Setting Up the Wireless AP Using Static Configuration](#) on page 199
- [Setting Up 802.1x Authentication for a Wireless AP](#) on page 203

AP Properties Tab - Basic Settings

Field	Description
Serial #	Read-only. Displays a unique identifier (serial number) that is assigned during the manufacturing process.
Host Name	Read-only. This value, which is based on AP Name, cannot be directly edited. This value depicts the AP Host-Name value. If the AP Name value does begin with a number, for example when it is the AP serial number, the AP model is prepended to the value. This value is used for tracking purposes on the <i>DHCP</i> server.
Name	The default value of the AP Name is the serial number, but it can be modified to any desired AP Name. Supported characters include: alphanumeric, blank space, hyphen, underscore, and period. Up to 255 characters.
Location	Define the location of the AP. When a client roams to an AP with a different location, Area Notification is triggered. The Area Notification feature is designed to track client locations within pre-defined areas using either the Location Engine (for more information, see Configuring the Location Engine on page 609) or the AP Location field. When the clients change areas, a notification is sent. Location functionality on the AP is useful when access to Extreme Management Center OneView is not available.
Zone	Zone is a label that can be sent to a RADIUS server in place of an AP BSSID in the called-station-id attribute. It can be easier to base authorization decisions on the zone label rather than on the BSSID. Each AP can have its own Zone label although it is often useful to assign the same Zone to multiple APs.
Description	Type comments for the AP.
Topology	Read only. The Topology name with which the AP is registered.
AP Environment	Select — Indoor or Outdoor. This property is available for outdoor APs only, indicating where the AP is deployed. The Outdoor APs can be deployed in both indoor and outdoor environments. AP placement should depend on the country of operation that is selected and the country regulatory domain requirements for radio emissions. For more information, see Outdoor Access Point Installation on page 167.

Field	Description
Hardware Type	<p>Select the hardware model of this AP from the drop-down menu. With ExtremeWireless v10.01 each controller is licensed in a specific domain. There are three types of domain licenses: FCC, ROW, EGY, and MNT. The ExtremeWireless user interface reflects the domain of the controller. The following are use cases for each domain:</p> <ul style="list-style-type: none"> • A wireless controller with an FCC license can manage AP37xx, AP38xx, and AP39xx-FCC. These access points can be deployed in the United States, Puerto Rico, or Colombia. • A wireless controller with a ROW license can manage AP37xx, AP38xx, and AP39xx-ROW. These access points can be deployed in any country <i>except</i> the United States, Puerto Rico, Egypt, or Colombia. • A wireless controller with a MNT license can manage only domain-locked access points, which are the AP39xx-FCC and the AP39xx-ROW only. The AP39xx-FCC must be deployed in the United States, Puerto Rico, or Colombia. The AP39xx-ROW must be deployed in any country <i>except</i> the United States, Puerto Rico, Egypt, or Colombia. <p>Note: The AP37xx and AP38xx <i>cannot</i> connect to a controller licensed in the MNT domain.</p> <ul style="list-style-type: none"> • A wireless controller with a EGY license can manage AP37xx, AP38xx, and AP39xx-EGY.
Application Version	Displays the ExtremeWireless release version.
Status	<p>Approved — Indicates that the AP has received its binding key from the controller after the discovery process.</p> <p>If no status is shown, that indicates that the AP has not yet successfully been approved for access with the secure controller.</p> <p>You can modify the status of an AP on the Access Approval screen. For more information, see Modifying the Status of a Wireless AP on page 156.</p>
Active Clients	Displays the number of wireless devices currently associated with the AP.

Field	Description
Role	<p>Displays the role for the AP.</p> <p>Note: You can only view these options here. You cannot change them.</p> <p>Options include:</p> <ul style="list-style-type: none"> • Traffic Forwarding — Normal Operation. Applies to all APs. • Guardian — Once the AP is configured as a Guardian, the AP stops forwarding traffic and dedicates both radios to threat detection and countermeasures. For more information, see Configuring an AP as a Guardian on page 221. The AP can be configured in one of three sub-modes: <ul style="list-style-type: none"> • Out-of-Service with its radios off • Providing full bridging functionality without RADAR • Providing full bridging functionality and In-Service RADAR. <p>For more information, see Configuring a Guardian Scan Profile on page 577.</p> <ul style="list-style-type: none"> • AirDefense Sensor — AP39xx integration with the AirDefense Services Platform (ADSP). Alternative to the Guardian AP configuration. For more information, see Configuring an AirDefense Profile on page 568.
Country	<p>Click the country of operation.</p> <p>Note: The antenna you select determines the available channel list and the maximum transmitting power for the country in which the AP is deployed.</p>

Related Links

[AP Properties Tab - Advanced Settings](#) on page 164

AP Properties Tab - Advanced Settings

Field	Description
Poll Timeout	<p>Type the timeout value, in seconds. The AP uses this value to trigger re-establishing the link with the Controller if the AP does not get an answer to its polling. The default value is 10 seconds.</p> <p>Note: If you are configuring session availability, the Poll Timeout value should be 1.5 to 2 times of Detect link failure value on AP Properties screen. For more information, see Session Availability on page 545.</p>
Secure Tunnel	<p>This feature, when enabled, provides encryption, authentication, and key management between the AP and/or controllers.</p> <p>Select the desired Secure Tunnel mode from the drop-down list:</p> <ul style="list-style-type: none"> • Disabled — Secure Tunnel is turned off and no traffic is encrypted. All SFTP/SSH/TFTP traffic works normally. • Encrypt control traffic between AP & Controller — An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control traffic is encrypted. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. • Encrypt control and data traffic between AP & Controller — This mode only benefits routed/bridged@Controller Topologies. An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control and data traffic is encrypted. The AP skips the registration and authentication phases, and when selected, the Secure Tunnel Lifetime feature can be configured. <p>Note: This option is not available for AP3805 models.</p> <ul style="list-style-type: none"> • Debug mode — An IPSEC tunnel is established from the AP to the controller, no traffic is encrypted, and all SFTP/SSH/TFTP traffic works normally. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. <p>Note: Changing a Secure Tunnel mode will automatically disconnect and reconnect the AP.</p>
Secure Tunnel Lifetime	<p>Available when Secure Tunnel is enabled. Enter an interval (in hours) at which time the keys of the IPSEC tunnel are renegotiated.</p> <p>Note: Changing the Secure Tunnel Lifetime setting will not cause any AP disruption.</p>
Enable SSH Access	Click to enable or disable SSH for access to the AP.
Enable location-based-service	Enable or disable the AeroScout, Ekahau, or Centrak location-based service for the AP.
Maintain client session in event of poll failure	Select this option (if using a bridged at AP VNS) if the AP should remain active if a link loss with the controller occurs. This option is enabled by default.
Restart service in the absence of controller	Select this option (if using a bridged at AP VNS) to ensure the AP's radios continue providing service if the AP's connection to the controller is lost. If this option is enabled, it allows the AP to start a bridged at AP VNS even in the absence of a controller.

Field	Description
Use broadcast for disassociation	<p>Select this option if you want the AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This affects the behavior of the AP under the following conditions:</p> <ul style="list-style-type: none"> • If the AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection). • If a BSSID is deactivated or removed on the AP. <p>This option is disabled by default.</p>
Enable LLDP	<p>Click to enable or disable the AP from broadcasting LLDP information. This option is disabled by default.</p> <p>If SNMP is enabled on the controller and you enable LLDP, the LLDP Confirmation dialog is displayed.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> • Proceed (not recommended) — Select this option to enable LLDP and keep SNMP running, and then click OK. • Disable SNMP publishing, and proceed — Select this option to enable LLDP and disable SNMP, and then click OK. • For more information on enabling SNMP, see the <i>ExtremeWireless Maintenance Guide</i>.
Announcement Interval	<p>If LLDP is enabled, type how often the AP advertises its information by sending a new LLDP packet. This value is measured in seconds.</p> <p>If there are no changes to the AP configuration that impact the LLDP information, the AP sends a new LLDP packet according to this schedule.</p> <p>Note: The Time to Live value cannot be directly edited. The Time to Live value is calculated as four times the Announcement Interval value.</p>
Announcement Delay	<p>If LLDP is enabled, type the announcement delay. This value is measured in seconds. If a change to the AP configuration occurs which impacts the LLDP information, the AP sends an updated LLDP packet. The announcement delay is the length of time that delays the new packet delivery. The announcement delay helps minimize LLDP packet traffic.</p>
IP Multicast Assembly	<p>Click to Enable or Disable IP Multicast Assembly on this Wireless AP. If Enabled, the IP Multicast Assembly feature assembles multicast data packets that were too large to fit the MTU size of the tunnel and were fragmented in order to fit the tunnel header. This feature is disabled by default.</p>
Active OBSS channel width adjustment	<p>When enabled, this setting avoids channel overlap by shrinking channels, when ACS detects an overlapping BSS.</p> <p>Before a radio provides service, it performs an overlapping BSS coexistence scan to ensure that the radio's channel will not overlap with a nearby operating AP's secondary channels. This behavior is in accordance with the 802.11 standard and provides data to the Channel Inspector Report.</p> <p>If the channel width is set to 40 or 80 MHz and an overlap is detected, ACS shrinks the channel to 20 or 40MHz to avoid the overlap.</p> <p>When this setting is disabled, the radio starts the service in spite of the overlap.</p> <p>By default, this option is enabled for newly deployed APs and is disabled for existing AP deployments, ensuring backward compatibility with previous ExtremeWireless releases.</p>
Balanced Channel List Power	<p>This simplifies power settings such that they will function across all channels in the channel plan.</p>

Field	Description
Low Power Mode Override	<p>Check this box to have AP ALWAYS operate in 4x4 mode regardless of what was negotiated with the Switch PoE. When this option is cleared, the AP operates in 2x2 or 4x4 depending on what was negotiated with the Switch PoE using the 2-event classification.</p> <ul style="list-style-type: none"> AP sends Power Status element with "Power Mode" set to 0 when "Low Power Mode Override" is enabled. AP sends Critical Log "entering Low Power mode" only if negotiated .af with Switch PoE and "Low Power Mode Override" is disabled. Otherwise, Critical Log is not sent. Controller "Network Health" shows only APs that have "Power Mode" bit in the Power Status set to 1. <p>The default configuration for the 39xx AP is disabled.</p>
LED	Select the desired LED pattern from the drop-down list. Options include: Off, WDS Signal Strength, Identify, and Normal.
Real Capture	<p>Click Start to start real capture server on the AP. Default capture server timeout is set to 300 seconds and the maximum configurable timeout is 1 hour. While the capture session is active, the AP interface operates in promiscuous mode.</p> <p>From the Wireshark GUI, set the capture interface to the IP address of the selected AP, and select null authentication. Once Wireshark connects to the AP, the AP's interfaces are listed as available to capture traffic. eth0 is the wired interface, wlan0 is the 5Ghz interface, and wlan1 is the 2.4Ghz interface. You can capture bidirectional traffic on eth0, wifi0, and wifi1. The capture on wifi0 and wifi1 does not include internally generated hardware packets by the capturing AP.</p> <p>The capturing AP does not report its own Beacons, Retransmission, Ack and 11n Block Ack. If this information is needed, perform Real Capture from a second AP that is close by. Make sure both APs are on the same wireless channel. Broadcast an SSID to activate the radios, but do not broadcast the SSID of the AP you are troubleshooting. You do not want the clients to connect to the second capturing AP.</p> <p>Capture statistics are found on the Active Wireless APs report (see Viewing Statistics for APs on page 627).</p>

Related Links

[AP Properties Tab - Basic Settings](#) on page 161

Professional Install Settings

The Professional Install option is only available for AP models with external antennas. The fields and corresponding antenna value options that appear on the **Professional Install** dialog depend on the selected AP and the antenna models that are available. Select an antenna for each available port. By default, the two antennas must be identical. However, you have the option to select **No Antenna** for the second antenna port. The AP3915e and AP3917e access point models offer an external IoT antenna. Select the antenna model from the drop-down field. Choose the desired attenuation for each radio from the drop-down list. Selectable range is from 0 to 30 dBI.

Professional install [?] [X]

Radio 1 Port 5G-1 Antenna Type⁴: No Antenna ▼

Radio 1 Port 5G-2 Antenna Type⁴: No Antenna ▼

Radio 2 Port 2.4G-1 Antenna Type⁴: No Antenna ▼

Radio 2 Port 2.4G-2 Antenna Type⁴: No Antenna ▼

⁴ Change of Antenna Type may cause AP to reboot.

IoT Antenna: No Antenna ▼

Radio1 Attenuation: 0 ▼

Radio2 Attenuation: 0 ▼

Close

Figure 30: Professional Install dialog AP3917

Outdoor Access Point Installation

The FCC regulations for the indoor and outdoor installation are different. The professional installer must configure the access point transmitters accordingly. Products that are specifically intended to be placed outdoors are configured at the factory for compliant outdoor operation. Professional installers should review the following to assess the legality of outdoor deployments:

- When a transmitter is placed indoors but the antenna is placed outdoors, the FCC interprets this as an outdoor installation.
- When a transmitter is placed indoors and the antenna is oriented to intentionally radiate outdoors, the FCC interprets this as an outdoor installation.
- When the transmitter is placed on a loading dock or inside a covered stadium with a retractable cover, the FCC views this as an outdoor installation.

Antenna Gain

Antenna gain is the ratio of an antenna's radiation intensity in a given direction to the intensity produced by a no-loss, isotropic antenna radiating equally in all directions. An antenna's gain along the horizon and at an elevation of 30 degree may vary. The elevation gain is defined as the maximum antenna gain at 30 to 150 degrees above the horizon. If elevation gain is configured, the transmit (TX) power calculations maximize the allowable TX power for an elevation below 30 degree.

Access Points must conform to U.S. Federal Communications Commission's (FCC) limitations. FCC has now stipulated a 21dBm Effective Isotropic Radiated Power (EIRP) limit for power directed 30 degrees above the horizon. For Extreme Networks -supplied antennas, compatible with 5.0 GHz on the access point, refer to the Antenna Guide for Elevation Gain information. If using a third-party antenna, you must obtain the antenna-elevation gain information from the antenna manufacturer.

The elevation gain should be configured if the access point:

- Is deployed outdoors, and

- Is used with a dipole antenna (Panel antennas and polarized antennas are for point to point only and are excluded from this requirement.) and
- Is transmitting in the 5.15 - 5.25 GHz Unlicensed National Information Infrastructure-1 (UNII-1) band.

Professional installers must complete the following steps to ensure compliance with the FCC rule:



Note

ExtremeWireless determines the antenna peak gain and elevation gain based on the user configured settings.

- 1 Configure the antenna type from the **Professional Install** dialog.
- 2 Configure the antenna placement from the **AP Environment** field on the **AP Properties** tab.
- 3 Configure the **Country** field on the **AP Properties** tab.

The firmware uses this information with hardcoded maximum limits (that are determined during testing) to limit the EIRP below 21dBm for outdoor use in UNII-1 band. For information on specific antennas, refer to the *ExtremeWireless External Antenna with Wave 2*.

Related Links

[AP Properties Tab - Basic Settings](#) on page 161

[Professional Install Settings](#) on page 166

[Outdoor Access Point Installation](#) on page 167

Assigning Wireless AP Radios to a VNS

The following describe methods of assigning AP radios to a VNS:

- **VNS configuration** — When a VNS is configured, you can assign AP radios to the VNS through its associated WLAN Service. For more information, see [Configuring WLAN Services](#) on page 318.



Note

To configure foreign AP radios to a VNS, use the VNS configuration method. Foreign APs are listed and available only for VNS assignment from the **WLAN Services** tab. For more information, see [Configuring a VNS](#) on page 390.

- **AP Multi-edit** — When you configure multiple APs simultaneously, use the AP Multi-edit feature. For more information, see [AP Multi-Edit Properties](#) on page 111 .
- **Wireless AP configuration** — When you configure an individual AP, assign its radios to a specific WLAN Service.

To assign wireless AP radios when configuring an AP:

- 1 From the top menu, click **AP**.
- 2 Click the appropriate AP in the list (not the check box). The **AP Details** dialog is displayed.
- 3 Click **Configure**.

The **AP Properties** tab is displayed.

- 4 Click the **WLAN Assignment** tab.

Edit AP
?
✕

[<Back](#)

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.1x
WLAN Name		Airtime %	Radio 1	Radio 2	
	CNL-412-0-0	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-0-1	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-0-2	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-0-3	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-1-2-wds	-	<input type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-1-4-wds	-	<input type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-1-5	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-1-6	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-1-7	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-2-10	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	CNL-412-2-11	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	CNL-412-2-12-wds	-	<input type="checkbox"/>	<input type="checkbox"/>	
	CNL-412-2-8	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	CNL-412-2-9	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	CNL-412-3-12	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	CNL-412-3-13	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Copy to Defaults
Reset to Defaults
Apply
Close



Note

Airtime % is available for AP38xx and AP39xx access point models that are assigned WLANs configured with Reserved Airtime.

- 5 In the **Radio 1** and **Radio 2** columns, select the radio check box that you want to assign for each WLAN Service.
- 6 To save your changes, click **Apply**.

Related Links

[Assigning WLAN Services to Client Ports](#) on page 170

[AP Properties Tab Configuration](#) on page 159

[Configuration Parameters for Radio Properties](#) on page 180

[Setting Up 802.1x Authentication for a Wireless AP](#) on page 203

[AP Multi-Edit Properties](#) on page 111

[Configuring Airtime Fairness: Reservation Mode](#) on page 406

NEW! Assigning WLAN Services to Client Ports

When configuring client ports on access point models AP391x that offer client ports, you can assign one or more client ports to a single WLAN service. Client ports offer 802.1x authentication and policy support.



Note

Network access for the AP3916ic camera function is controlled through policy definition, assigned as a the CAM port. The camera port on the AP3916 is treated as a wired client port.

- 1 From the top menu, click **AP**.
- 2 Select a specific AP.

Port options depend on the AP model you select:

- AP3912 supports wired client ports 1-3.
- AP3916ic supports the wired CAM port for a camera.
- AP3917i/e supports 1 client port.
- Additionally, all the AP391x models, including AP3915i/e, support IoT Thread Gateway using the AP as a border gateway router.

The **AP Properties** dialog appears.

- 3 Click **Configure**.
- 4 Select the **WLAN Assignment** tab.
- 5 Select one or more client ports for each WLAN Service.

All Port Assignments:

- One WLAN can be assigned per port. The assignment enables the port.
- Wireless and wired users associated to the same WLAN service receive identical service. They are affected by the same policies and filters.

The wired ports for the AP391x default to auto-negotiation for speed and mode. To configure fixed speed and mode values (for instance, 100Mbps and Full Duplex), select the **Static Configuration** tab and select the speed and mode settings for the Ethernet port and each client port. Configure the values that the client hardware supports.

Edit AP [?] [X]

[<Back](#)

AP Properties | WLAN Assignment | Radio 1 | Radio 2 | IoT | **Static Configuration** | 802.1x

[Changing static configuration settings may cause the AP to reboot. Reboots caused by static configuration changes may make the AP unreachable from this EWC.]

VLAN Settings

Tagged - VLAN ID: (1-4094)

Untagged

IP Address Assignment

Use DHCP

Static Values

IP Address:

Netmask:

Gateway:

Ethernet Port

Ethernet Speed: Tunnel MTU:

Ethernet Mode:

Client Ports

P1

P2

P3

Wireless Controller Search List

Up

Down

Delete

Copy to Defaults | Reset to Defaults | Apply | Close

Figure 31: Port Configuration for AP3912 Wired Ports

CAM Port Assignments:

- The topology associated with the role that is assigned to the CAM port (either through WLAN assignment or through device MBA authentication) must be configured to allow ONVIF camera discovery and video streaming. Configure the default topology to explicitly allow multicast bridging of WS-Discovery group (239.255.255.0).
- When the camera port is unassigned, it is disabled, and the camera is disconnected from the network and turned off.
- One policy definition for wired and wireless users. Users on wired ports can receive the same default policy. However, the camera function (CAM) can be assigned a specific device policy to separate user service and video surveillance networks.
- The camera function can be assigned to B@AP and B@AC topologies and Mac Based Authentication for dynamic policies.

- Configure MAC authentication (MBA) for network attached devices or collect device metrics through RADIUS accounting from the **Auth&Acct** tab.
- WLAN SSID, Privacy, and QoS settings are not relevant for the camera functionality.
- Captive Portal and 802.1x are not supported on the CAM port.



Note
Bind the WLAN Service to the VNS to activate service.

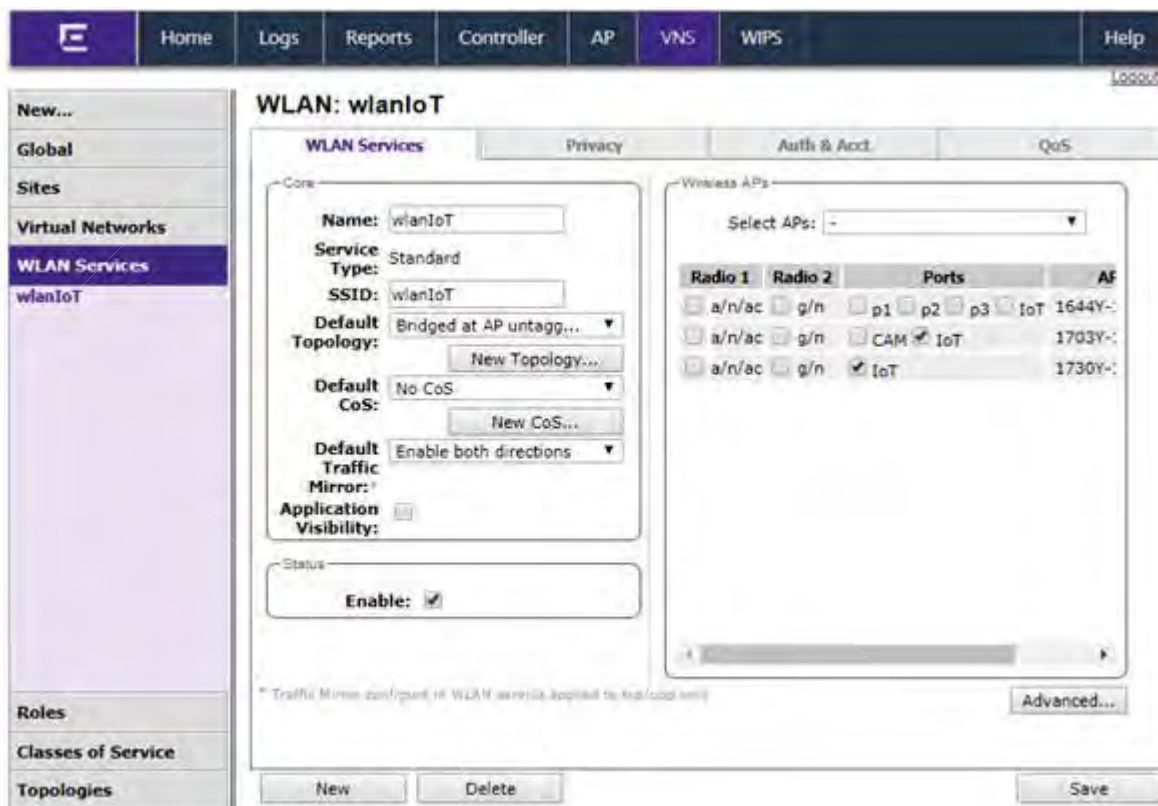


Figure 32: WLAN Services Port Assignment

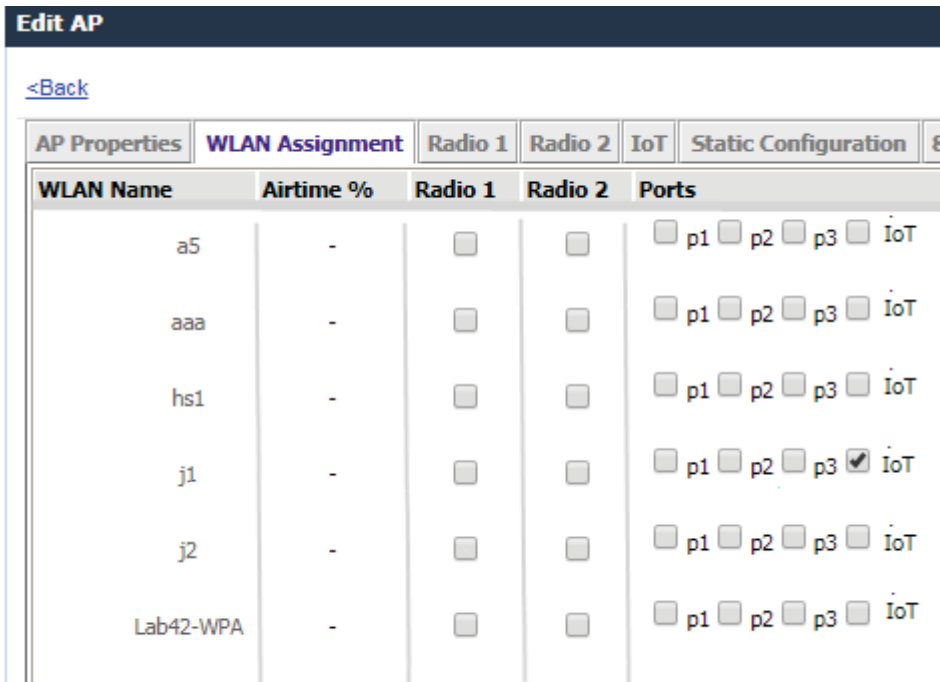


Figure 33: Assigning Ports to WLAN Service on the AP3912

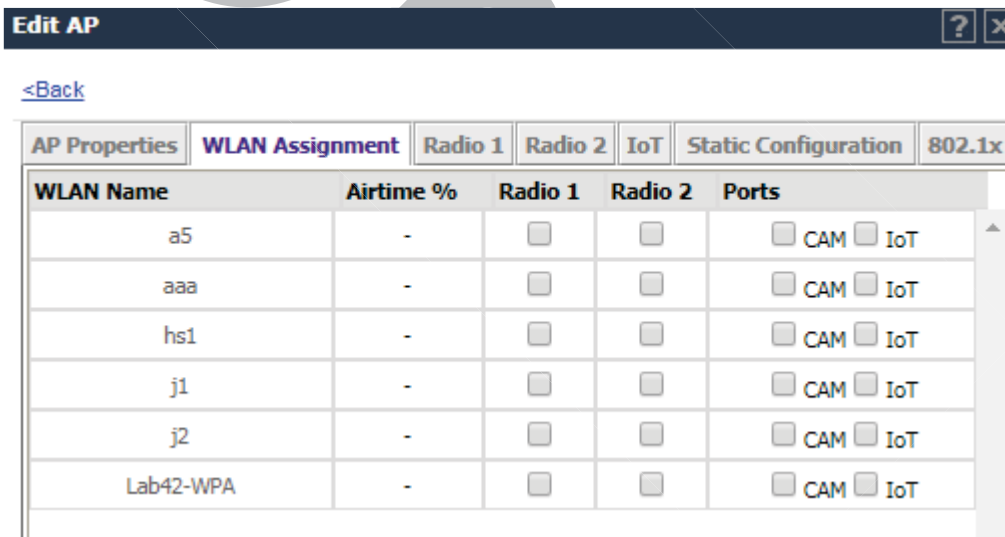


Figure 34: Assigning the Camera Port to WLAN Service on the AP3916ic

The screenshot shows the 'Edit AP' configuration window with the 'WLAN Assignment' tab selected. The table below shows the configuration for two WLANs:

WLAN Name	Airtime %	Radio 1	Radio 2	Ports
a1	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> IoT
Lab46-WPA	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> IoT

Buttons at the bottom: Copy to Defaults, Reset to Defaults, Apply, Close.

Figure 35: Assigning the IoT Port to WLAN Service on the AP3915

Related Links

- [Configuring IoT Applications](#) on page 189
- [Setting Up the Wireless AP Using Static Configuration](#) on page 199
- [Configuring Common Configuration Default AP Settings](#) on page 135

Configuring Wireless AP Radio Properties

Wireless AP radio properties can vary depending on the model of the AP being configured. For specific information on modifying a wireless 802.11n AP, see [Modifying 11n and 11ac Wireless AP Radio Properties](#) on page 178.

Dynamic Radio Management (DRM)

Use the Dynamic Radio Management (DRM) controller function to establish the optimum radio configuration for your APs.

Consider the following deployment methodologies:

- Plan the wireless RF deployment using various site survey methodologies including the ExtremeCloud RF planner. Configure each AP's channel width and channel according to the RF plan.
- Use the DRM automatic tool to configure the deployed AP's channel width and channel according to the channel plan.
 - Use DRM Auto Channel Selection (ACS) to automatically assign the APs to appropriate channels and channel width.
 - Use Auto Tx Power Control (ATPC) to set transmit power and let the AP dynamically adapt transmit power.
 - Use Dynamic Channel Selection (DCS) to monitor channel occupancy around the APs and optionally allow the AP to dynamically adapt the channel.

The controller's DRM functionality:

- Adjusts transmit power levels to balance coverage between APs assigned to the same RF domain and operating on the same channel.
- Triggers ACS for all selected APs in the deployment, simultaneously. The APs determine the deployment density and the optimal channel width for the selected group.

Density deployment is based on the following factors:

- The number of channels configured in the channel list
- The number of APs that have to be set up
- The number of detected APs that do not belong to the deployment.

Each AP is set to the best available channel. The channel inspector displays the RF environment seen by each AP. Use the Channel Inspector Report to understand why an AP selects a channel and, if necessary, to make manual adjustments.

AP39xx and AP38xx perform overlapping BSS (OBSS) scan every time the radio is restarted. This scan results are used as follows:

- Channel inspector is always updated with the latest RF environment seen by the AP.
- If the channel width is set to 40MHz or 80MHz and the AP property **Active OBSS channel width adjustment** is enabled, the AP shrinks its channel to avoid overlapping with other APs detected in the area. (An OBSS overlap occurs when a primary channel and a secondary channel overlap.) After the interfering AP is shut down and the AP's radio is reset, the channel width returns to 40MHz or 80MHz.

Note



When setting a fixed channel width to 40 MHz or 80 MHz, the **Active OBSS channel width adjustment** setting must be disabled. This setting is disabled by default for existing APs in order to maintain existing behavior and the existing channel plan. For APs that are newly added to the network, this setting is enabled by default.

- AP39xx and AP38xx return to original channel after a RADAR event in order to restore original channel plan.

When a RADAR event is detected, the channel is marked and the AP selects a new channel from the allowed channel list. After 30 minutes, if there are no clients associated with the AP, the AP returns to the original channel. If there are associated clients, the AP tries to return to the original channel every five minutes until there are no clients associated with the radio.

The DRM feature consists of three functions:

Auto Channel Selection (ACS)

ACS provides an easy way to optimize channel arrangement based on the current situation in the field. An optimal solution is provided only if ACS is triggered on all APs in a deployment, or all APs placed in a distinct area like a floor. ACS forces the channel width selection of the involved APs to Auto width. The ACS algorithm selects the optimal channel width for all the selected APs and places each AP on the best channel available in its area. Use the Channel Inspector Report to visualize why the AP was placed on the selected channel.

Triggering ACS on a single AP or on a subset of APs can be useful but it is not an optimal solution. The ACS algorithm places the selected APs as best it can considering the channels occupied by other

operating APs. ACS relies on the RF channel information observed at the time it is triggered. Once an AP has selected a channel, it remains operating on that channel until you change the channel or trigger ACS again.

ACS can be triggered by one of the following events:

- A new AP registers with the controller and the **AP Default Settings** channel is **Auto**.
- A user selects **Auto** from the **Request New Channel** drop-down list on the Wireless AP's radio configuration tabs.
- A user selects **Auto** from the **Channel** drop-down list on the **AP Multi-edit** screen.
- If Dynamic Channel Selection (DCS) is enabled in active mode and a DCS threshold is exceeded.
- A Wireless AP detects radar on its current operating channel and it employs ACS to select a new radar free channel. The AP returns to the original channel under the following condition:
 - A 30-minute Non-Occupancy timer expired per the DFS standard.
 - The AP does not disrupt service to any clients.
- You can initiate ACS from the Channel Inspector Report.
- ACS is triggered for Site deployments or Cloud deployments by sending the ACS command to one of the member APs, which will distribute the ACS command to all other member APs. Each Site is considered an RF domain.
- Channel Plan — The ACS algorithm selects channels from the configured channel plan. You can define the channel plan for each AP or accept the default plan. It is recommended that all APs in a deployment have identical channel plans. Defining a channel plan allows you to limit the available channels for use during an ACS scan. For example, you may want to avoid using specific channels because of allowed power limits on that channel or regulatory domain, or avoid DFS channel RADAR interference.
- Multi-Edit — The best way to trigger ACS between multiple APs is to use the AP Multi Edit option. First, select Radio 1 or Radio 2 actions, and then select **Auto Channel Select**. APs that configure ACS together, must all be part of the same RF domain. Therefore, set the RF Domain before ACS is started. ACS between multiple APs must start at the same time.

Dynamic Channel Selection (DCS)

DCS allows a Wireless AP to monitor RF channel conditions and noise levels on the channel on which the AP is currently operating. DCS can operate in the following modes:

- **Monitor** — When DCS is enabled in monitor mode the AP monitors channel occupancy and traffic or noise levels on the channel on which the AP is currently operating. The DCS monitor alarm and generated stats can be used to evaluate the RF environment of your deployed APs.
- **Active** — When DCS is enabled in active mode and channel occupancy traffic or noise levels exceed the configured DCS thresholds, ACS is triggered to move the AP from a busy / noisy channel to the best available channel. Also, an alarm is triggered and an information log is generated.



Note

If DCS is enabled, DCS statistics can be viewed in the **Wireless Statistics by Wireless APs** display. For more information, see [Working with Reports and Statistics](#) on page 621.

Related Links

[AP Properties Tab - Advanced Settings](#) on page 164

[Use Cases for Dynamic Radio Management](#) on page 178

[Configuration Parameters for Radio Properties](#) on page 180

[AP Multi-Edit Properties](#) on page 111

[Radio Advanced Properties](#) on page 184

[Channel Inspector Report](#) on page 637

ATPC

The purpose of ATPC is to automatically adjust the coverage cell around an AP. During initial deployment, the Tx Power of each AP is adjusted to provide coverage without overlapping the coverage cell of a neighboring AP. To maintain optimal performance, it is important to maintain a small cell sizes to encourage WLAN clients to roam to the closest AP and operate at high data rates. This practice frees the channel as fast as possible and reduces congestion.

Setting the AP transmit power too high can cause interference and potentially exceed useful bounds. Setting the AP transmit power too low may introduce coverage gaps in the installation.

ATPC operates over a group of APs configured to participate in the same RF domain. Configure the **RF Domain** parameter as a unique string across all the APs that provide service coverage, ensuring that cell shaping is not influenced by non-participating APs. ATPC operates by periodically broadcasting custom probe requests that allow the other APs in range to determinate the “RF Distance / Path Loss” to the sending AP. Every 10 seconds, each AP evaluates the Path Loss to its neighbors. If Path Loss is less then 70dB, the AP reduces its Tx Power. If the Path Loss is more than 70dB, the AP boosts its Tx Power.

When all APs are operating, the cells size of each AP is adjusted to cover the surrounding area. If one AP fails, the APs around it increase their Tx Power, increasing the cell size, and compensating for the loss of the failed AP. If an RF obstructing object is moved between the APs, the APs increase Tx Power in order to maintain coverage.

The ATPC feature is configured for each radio. When you check **Auto Tx Power Ctrl (ATPC)** check box, you are enabling the radio to participate in the AP group that collaborates to automatically adjust the cell size. When ATPC is enabled, the following parameters are available for configuration:

- Max Tx Power
- Min Tx Power
- Auto Tx Power Ctrl Adj

The Max and Min Tx Power parameters set the power range used by the ATPC. The Auto Tx Power Ctrl Adj parameter allows you to manually adjust the Tx Power calculated by the ATPC algorithm (either up or down). The **Current Tx Power Level** field on the AP / Radio page displays the actual AP Tx Power.

ATPC preserving Power Setting — In some cases operators may use ATPC to initially set up the power setting of the APs over a service area, but then want to “freeze” this setting during normal operation of the network. When the **Auto Tx Power Ctrl (ATPC)** check box is cleared you have two choices:

- Maintain the ATPC-acquired Tx Power value after turning ATPC off.
- Set the Tx Power to the Max Tx Power value.

The ATPC feature allows you to use ATPC to achieve a Tx Power level required for the installation, and then statically maintain this value if ATPC is turned off.

Related Links

[Configuration Parameters for Radio Properties](#) on page 180

Use Cases for Dynamic Radio Management

The following scenarios outline use cases for Dynamic Radio Management (DRM).

- **Using ACS with a set of APs**

When you trigger ACS for a set of APs, the channel width is automatically set to Auto and ACS determines the deployment density and the desired channel width to minimize co-channel interference. A channel plan is created with non-overlapping cells, and each AP performs an overlapping BSS (OBSS) scan to avoid channel overlap.

- **Manually Selecting Channels and Channel Width**

When you select a fixed channel and channel width, the AP radio is set to the requested channel and width. The AP performs an overlapping BSS (OBSS) scan and sends the results to the Channel Inspector. If the setting **Active OBSS channel width adjustment** is not enabled, the radio uses the manually selected channel and width, and the detected overlap is not remedied automatically.

If **Active OBSS channel width adjustment** is enabled, the detected overlap is corrected by shrinking the channel width before the radio is enabled. The channel width can recover after a subsequent radio reset if the OBSS scan does not detect another channel overlap.

Modifying 11n and 11ac Wireless AP Radio Properties

The ExtremeWireless 37xx/W78xC series are 802.11n-compliant access points. AP38xx and AP39xx series are 11n and 11ac-compliant. This section describes how to configure/modify properties of an 11n or 11ac AP.

Channel Bonding

Channel bonding improves the effective throughput of the wireless LAN. In contrast to legacy APs which use radio channel spacings that are only 20 MHz wide, 11n wireless APs can use two channels at the same time to create a 40 MHz wide channel. 11ac wireless APs can use four channels at the same time to create an 80 MHz wide channel.

The 40 MHz channel width is achieved by bonding the primary channel (20 MHz) with an extension channel.

Channel bonding is predefined on both Radio 1 and Radio 2. Channel bonding is enabled by selecting the **Channel Width** on the **Radio** tabs. When selecting **Channel Width**, the following options are available:

- **20 MHz** — Channel bonding is not enabled:
 - 802.11n clients use the primary channel (20 MHz)
 - Non-802.11n clients, as well as beacons and multicasts, use the 802.11a/b/g radio protocols.
- **40 MHz** — Channel bonding is enabled:
 - 802.11n clients that support the 40 MHz channel width can use 40 MHz, 20 MHz, or the 802.11a/b/g radio protocols.

- 802.11n clients that do not support the 40 MHz channel width can use 20 MHz or the 802.11a/b/g radio protocols.
- Non-802.11n clients, beacons, and multicasts use the 802.11a/b/g radio protocols.
- **80 MHz** — Channel bonding is enabled:
 - 802.11ac clients that support the 80 MHz channel width can use 80 MHz, 40 MHz, 20 MHz, or the 802.11a/b/g radio protocols.
 - 802.11n clients that do not support the 80 MHz channel width can use 20 MHz, 40 MHz, or the 802.11a/b/g radio protocols.
 - Non-802.11n clients, beacons, and multicasts use the 802.11a/b/g radio protocols.
- **Auto** — Channel bonding is automatically enabled or disabled, switching between 20 MHz, 40 MHz, and 80 MHz, depending on how busy the extension channel(s) are. If the extension channel is busy above a prescribed threshold percentage, which is defined in the **40 MHz Channel Busy Threshold** box, channel bonding is disabled.

Channel Selection — Primary and Extension

The primary channel of the wireless 802.11n AP is selected from the **Request New Channel** drop-down list. If auto is selected, the ACS feature selects the primary channel. The channels in the **Request New Channel** drop-down list show which extension channel(s) are being used for bonding.

Guard Interval

The guard intervals ensure that individual transmissions do not interfere with one another. The wireless 802.11n AP provides a shorter guard interval that increases the channel throughput. You can select the guard interval to improve the channel efficiency. The guard interval is selected from the **Guard Interval** drop-down list. Longer guard periods reduce the channel efficiency.

Aggregate MSDU and MPDU

The wireless 802.11n AP provides aggregate Mac Service Data Unit (MSDU) and aggregate Mac Protocol Data Unit (MPDU) functions, which combine multiple frames together into one larger frame for a single delivery. This aggregation reduces the overhead of the transmission and results in increased throughput. The aggregate methods are enabled and defined selected from the **Aggregate MSDUs** and **Aggregate MPDUs** drop-down lists.

Antenna Selection

Wireless APs have differing numbers of antennas, internal or external, depending on the AP model.

Wireless APs by default transmit on all antennas. Depending on your deployment requirements, you can configure the AP to transmit on specific antennas. You can configure the wireless 802.11ac AP to transmit on specific antennas for both radios, including all the available modes:

- **Radio 1** — a/n/ac, ac-strict modes
- **Radio 2** — b/g, g/n, b/g/n, n-strict modes

When you configure the AP to use specific antennas, the following occurs:

- Transmission power is recalculated — The **Current Tx Power Level** value for the radio is automatically adjusted to reflect the recent antenna configuration. It takes approximately 30 seconds for the change to the **Current Tx Power Level** value to be reflected in the Wireless Assistant.

- Radio is reset — The radio is reset causing client connections on this radio to be lost.

To modify wireless AP radio properties:

- 1 From the top menu, click **AP**.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **Radio** tab you want to modify.

Configuration Parameters for Radio Properties

Table 15: Radio Properties

Field	Description
Base Settings	
BSS Info	BSS Info is read-only. After WLAN Service configuration, the Basic Service Set (BSS) section displays the MAC address on the AP for each WLAN Service and the SSIDs of the WLAN Services to which this radio has been assigned.
Admin Mode	Select On to enable the radio; select Off to disable the radio.
Radio Mode - Radio 1	<p>Note: Depending on the radio modes you select, some of the radio settings may not be available for configuration. The AP hardware version dictates the available radio modes.</p> <p>Click one of the following radio options for Radio 1:</p> <ul style="list-style-type: none"> • a — Click to enable the 802.11a mode of Radio 1 without 802.11n capability. • a/n — Click to enable the 802.11a mode of Radio 1 with 802.11n capability. • a/n/ac — Click to enable the 802.11ac mode of Radio 1 with 802.11ac capability. • ac-strict — Click to enable the 802.11ac mode of Radio 1 with 802.11ac strict capability. • n-strict — Click to enable the 802.11a mode of Radio 1 with 802.11n strict capability.

Table 15: Radio Properties (continued)

Field	Description
Radio Mode - Radio 2	<p>Note: Depending on the radio modes you select, some of the radio settings may not be available for configuration.</p> <p>Click one of the following radio options for Radio 2:</p> <ul style="list-style-type: none"> • b – Click to enable the 802.11b-only mode of Radio 2. If selected, the AP uses only 11b (CCK) rates with all associated clients. • g – Click to enable the 802.11g-only mode of Radio 2. • b/g – Click to enable both the 802.11g mode and the 802.11b mode of Radio 2. If selected, the AP uses 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients and will not transmit or receive 11n rates. • g/n – Click to enable both the 802.11g mode and the 802.11n mode of Radio 2. If selected, the AP uses 11n and 11g-specific (OFDM) rates with all of the associated clients. The AP will not transmit or receive 11b rates. • b/g/n – Click to enable b/g/n modes of Radio 2. If selected, the AP uses all available 11b, 11g, and 11n rates. • n-strict – Click to enable the 802.11n-strict mode of Radio 2. If selected, the AP can be configured to use 11n-strict rates with all of the associated clients. With n-strict mode enabled, the AP does not transmit or receive 11b or 11g rates.
Basic Radio Settings	
RF Domain	Type a string that uniquely identifies a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 16 characters. The RF Domain is used to identify a group of APs. The RF Domain feature is part of the Auto Tx Power Control (ATPC) feature (for more information, see Configuring Wireless AP Radio Properties on page 174).
Current Channel	Read-only. The actual channel the ACS has assigned to the AP radio. The Current Channel value and the Last Requested Channel value may be different because the ACS automatically assigns the best available channel to the AP, ensuring that a AP's radio is always operating on the best available channel.
Last Requested Channel	Read-only. The last wireless channel that you had selected to communicate with the wireless devices.
Request New Channel	<p>Click the wireless channel you want the wireless AP to use to communicate with wireless devices.</p> <p>Weather channels (116, 120, 124, 128) are supported for European compliance. See Channel Plan.</p> <p>Click Auto to request the ACS to search for a new channel for the AP, using a channel selection algorithm. This forces the AP to go through the auto-channel selection process again.</p> <p>Note: ACS in the 2.4 GHz radio band with 40 MHz channels is not recommended due to severe co-channel interference.</p> <p>Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, refer to the appropriate AP Installation Guide.</p>

Table 15: Radio Properties (continued)

Field	Description
Auto Tx Power Ctrl (ATPC)	<p>Click to either enable or disable ATPC from the Auto Tx Power Ctrl drop-down list. ATPC automatically adapts transmission power signals according to the coverage provided by the AP. After a period of time, the system stabilizes itself based on the RF coverage of your Wireless APs.</p> <p>Note: When enabled, Min Tx Power and Auto Tx Power Ctrl Adjust parameters can be edited, and the ATPC algorithm will adjust the AP power between Max Tx power and Min Tx Power. When disabled, the Max Tx Power selected value or the largest value in the compliance table will be the power level used by the radio, whichever is smaller.</p>
Current Tx Power Level	The actual Tx power level used by the AP radio.
Max Tx Power	<p>Displays dynamic power level based on channel selected. Select the Max TX Power from the drop-down list. The values in the Max TX Power drop-down are in dBm and will vary by AP. The values are governed by compliance requirements based on the country, radio, and antenna selected. Changing this value below the current Min Tx Power value will change the Min Tx Power to a level lower than the selected Max TX Power.</p> <p>Note: If Auto Tx Power Ctrl (ATPC) is disabled, the selected value or the largest value in the compliance table will be the power level used by the radio, whichever is smaller.</p>
Min Tx Power	<p>If ATPC is enabled, select the minimum Tx power level that is equal or lower than the maximum Tx power level. Extreme Networks recommends that you use 0 dBm if you do not want to limit the potential Tx power level range that can be used.</p> <p>Note: The Min Tx Power setting cannot be set higher than the Max Tx Power setting.</p>
Auto Tx Power Ctrl Adjust	<p>The Auto Tx Power Ctrl Adj parameter is a correction parameter that allows you to manually adjust (up or down) the Tx Power calculated by the ATPC algorithm. If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended that you use 0 dBm during the initial configuration. If you have an RF plan that recommends Tx power levels for each AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the Auto Tx Power Ctrl Adjust value to achieve the recommended values. Valid range is from - (Max Tx Power - Min Tx Power) dB to (Max Tx Power - Min Tx Power) dB.</p>

Table 15: Radio Properties (continued)

Field	Description
Channel Plan - Radio 1	<p>If ACS is enabled you can define a channel plan for the AP. Defining a channel plan allows you to control which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference.</p> <ul style="list-style-type: none"> • For 5 GHz Radio nodes, click one of the following: <ul style="list-style-type: none"> • All channels — ACS scans all channels for an operating channel and, when ACS is triggered, the optimal channel is selected from all available channels. • All Non-DFS Channels — ACS scans all non-DFS channels for an operating channel. With ACS, the AP selects the best non-DFS channel. • Custom — To configure individual channels from which the ACS selects an operating channel, click Configure. The Custom Channel Plan dialog displays. By default, all channels participate in the channel plan. Click the individual channels you want to include in the channel plan. To select contiguous channels, use the Shift key. To select multiple, non-contiguous channels in the list, use the CTRL key. Click OK to save the configuration. • All channels including weather radar — ACS selects the best channel from the available channels list. Selected channel may be DFS, weather-radar DFS or non-DFS. Weather-radar channels are approved for selected AP models in selected countries. Consult the compliance information for the selected AP. <p style="margin-left: 20px;">The weather channel includes 5600-5650MHz sub-bands and requires a listening period before the AP can provide wireless service. During the listening period, the Current Channel field for DFS channels displays the value <i>DFS Timeout</i>, and the weather channel fields display <i>DFS Timeout</i> . In Europe, the listening period can be up to 10 minutes. In the U.S., this period is 1 minute.</p> • For 2.4 GHz Radio nodes, click one of the following: <ul style="list-style-type: none"> • 3 Channel Plan — ACS scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in the rest of the world. • 4 Channel Plan — ACS scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world. • Auto — ACS scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world. • Custom — If you want to configure individual channels from which the ACS selects an operating channel, click Configure. The Add Channels dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click OK.

Table 15: Radio Properties (continued)

Field	Description
Channel Plan - Radio 2	<p>If ACS is enabled, you can define a channel plan for the AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference. Click one of the following:</p> <ul style="list-style-type: none"> • 3 Channel Plan — ACS 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 — ACS 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 — ACS 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. • Custom — If you want to configure individual channels from which the ACS selects an operating channel, click Configure. The Add Channels dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click OK.
View	Click to open a new dialog that displays the selected Channel Plan for the antenna.

Related Links

[Radio Advanced Properties](#) on page 184

[Radio Actions](#) on page 130

[AP Properties Tab Configuration](#) on page 159

[Assigning Wireless AP Radios to a VNS](#) on page 168

[Setting Up the Wireless AP Using Static Configuration](#) on page 199

[Setting Up 802.1x Authentication for a Wireless AP](#) on page 203

*Radio Advanced Properties***Table 16: Advanced Radio Properties**

Field	Description
Advanced Dialog - Base Settings	
DTIM period	Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. Use a small number to minimize broadcast and multicast delay. The default value is 5.
Beacon Period	Defines the time, in milliseconds, between beacon transmissions. The default value is 100 milliseconds.
RTS/CTS Threshold	Type the packet size threshold, in bytes, above which the packet is preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is 2346, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.

Table 16: Advanced Radio Properties (continued)

Field	Description
Frag. Threshold	Type the fragment size threshold, in bytes, above which the packets are fragmented by the AP prior to transmission. The default value is 2346, which means all packets are sent unfragmented. Reduce this value only if necessary.
Maximum Distance	Enter a value from 100 to 15,000 meters that identifies the maximum link distance between APs that participate in a WDS. This value ensures that the acknowledgement of communication between APs does not exceed the timeout value predefined by the 802.11 standard. The default value is 100 meters. If the link distance between APs is greater than 100 meters, configure the maximum distance up to 15,000 meters so that the software increases the timeout value proportionally with the distance between APs. Do not change the default setting for the radio that provides service to 802.11 clients only.
Advanced Dialog - Basic Radio Settings	
Dynamic Channel Selection	To enable Dynamic Channel Selection, click one of the following: <ul style="list-style-type: none"> • Monitor Mode — If enabled, a selection of DCS Interference Events appears in a separate dialog. If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. • Active Mode — If enabled, a selection of DCS Interference Events appears in a separate dialog. If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the AP ceases operating on the current channel and ACS is employed to automatically select an alternate channel for the AP to operate on.
Probe Suppression	Click to Enable Probe Suppression. <ul style="list-style-type: none"> • Forced Disassociate — Click to enable. • RSS Threshold — 90 (Range of -50 to -100). Applies to AP37xx, AP38xx, and AP39xx series APs.
Min. Basic Rate	Click the minimum data rate that must be supported by all stations in a BSS: 6, 12, or 24 Mbps and MCS0-MCS7 for n Radio (MCS0, 1 to MCS7,1 for a/n/c radio). If necessary, the Max Basic Rate choices adjust automatically to be higher or equal to the Min Basic Rate.
Advanced Dialog - Multicast Settings	
Max % of non-unicast traffic per Beacon period	Enter the maximum percentage of time that the AP transmits non-unicast packets (broadcast and multicast traffic) for each configured Beacon Period. For each non-unicast packet transmitted, the system calculates the airtime used by each packet and drops all packets that exceed the configured maximum percentage. By restricting non-unicast traffic, you limit the impact of broadcasts and multicasts on overall system performance.
Optimized for power save	Click to optimize for power save.
Adaptable rate	Click to enable adaptable rate capabilities.
Multicast to Unicast delivery	Click to set the Multicast to Unicast delivery method from the drop-down list.

Table 16: Advanced Radio Properties (continued)

Field	Description
Advanced Dialog - 11n Settings	
Guard Interval	Intended to eliminate interference between symbols during transmission. It is the space between the symbols being transmitted. Valid values are Long or Short. Enabling Short Guard Interval increases throughput, but can increase interference. Enabling Long Guard Interval can increase overhead due to additional idle time.
Protection Mode	Click a protection mode: None, Auto, or Always. The default and recommended setting is Auto. Click None if 11b APs and clients are not expected. Click Always if you expect many 11b-only clients.
Extension Channel Busy Threshold	Click a protection type, CTS Only or RTS CTS, when a 40 MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
Aggregate MSDUs	Click an aggregate MSDU mode: Enabled or Disabled. Aggregate MSDU increases the maximum frame transmission size.
Aggregate MPDUs	Click an aggregate MPDU mode: Enabled or Disabled. Aggregate MPDU provides a significant improvement in throughput.
Aggregate MPDU Max Length	Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes. For the 802.11ac radio (Radio 1 of the AP38xx), the range is 1024-1048575.
Agg. MPDU Max # of Sub-frames	Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
ADDBA Support	Click an ADDBA support mode: Enabled or Disabled. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. ADDBA Support must be enabled if Aggregate APDU is enable.
LDPC	Click an LDPC mode: Enabled or Disabled. LDPC increases the reliability of the transmission resulting in a 2dB increased performance compared to traditional 11n coding.
STBC	Click an STBC mode: Enabled or Disabled. 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 are enabled for single stream rates.
TXBF	Tx Beam Forming is a technique of re-aligning the transmitter multipath spatial streams phases in order to get better signal-to-noise ratio on the receiver side. Click a TXBF mode: For the AP37xx and AP38xx models, valid values are Enabled or Disabled. For the 39xx APs, this setting is only available on Radio1 and valid values are MU-MIMO and Disabled.
Advanced Dialog - 11b Settings	
Preamble	Click a preamble type for 11b-specific (CCK) rates: Short or Long. Click Short if you are sure that there is no pre-11b AP or a client in the vicinity of this wireless AP. Click Long if compatibility with pre-11b clients is required.
Advanced Dialog - 11g Settings	

Table 16: Advanced Radio Properties (continued)

Field	Description
Protection Mode	Click a protection mode: None, Auto, or Always. The default and recommended setting is Auto. Click None if 11b APs and clients are not expected. Click Always if you expect many 11b-only clients.
Protection Rate	Click a protection rate: 1, 2, 5.5, or 11 Mbps. The default and recommended setting is 11. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than 11 Mbps are required to ensure coverage.
Protection Type	Click a protection type: CTS Only or RTS CTS . The default and recommended setting is CTS Only. Click RTS CTS only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment. The overall throughput is reduced when Protection Mode is enabled, due to the additional overhead caused by the RTS/CTS. The overhead is minimized by setting Protection Type to CTS Only and Protection Rate to 11 Mbps. The overhead causes the overall throughput to be sometimes lower than if just 11b mode is used. If there are many 11b clients, it is recommended that you disable 11g support (11g clients are backward compatible with 11b APs). An alternate approach, although potentially a more expensive method, is to dedicate all APs on a channel for 11b (for example, disable 11g on these APs) and disable 11b on all other APs. The difficulty with this method is that the number of APs must be increased to ensure coverage separately for 11b and 11g clients.

Achieving High Throughput with 11n and 11ac Wireless APs

To achieve high throughput with the wireless APs, configure your system as described in this section.



Note

Some client devices choose a 2.4 GHz radio even when a 5 GHz high-speed radio network is available. You may need to force those client devices to use only 5 GHz if you have configured high throughput only on the 5 GHz radio.

To achieve high throughput with a wireless AP:

- 1 From the top menu, click **AP**.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.

4 For **Radio 2** configure the following:

- In the **Radio Mode** drop-down list, click **b/g/n**.
- In the **Channel Width** drop-down list, click **40 MHz**.
- Under Advanced Settings, in the **Guard Interval** drop-down list, click **Short**.
- In the **11g Settings** section, click **None** in the **Protection Mode** drop-down list.



Note

Do not disable 802.11g protection mode if you have 802.11b or 802.11g client devices using this AP. Instead, configure only Radio 1 for high throughput unless it is acceptable to achieve less than maximum 802.11n throughput on Radio 2.

- If only 802.11n devices are present, disable 11n protection and 40 MHz protection:
 - **Protection Mode** — Click **None**.
 - **Protection Type** — Click **CTS only** or **RTS CTS**.



Note

Do not disable 802.11n protection mode if you have 802.11b or 802.11g client devices using this AP. Instead, configure only Radio 1 for high throughput unless it is acceptable to achieve less than maximum 802.11n throughput on Radio 2.

- **Aggregate MSDUs** — Click **Enabled**.
- **Aggregate MPDUs** — Click **Enabled**.
- **Aggregate MPDUs Max Length** — Click **65535** (for the 802.11ac AP models).
- **Agg. MPDUs Max # of Sub-frames** — Type **64**.
- **ADDBA Support** — Click **Enabled**.

5 Click the **Radio 1** tab, and then do the following:

- In the **Admin Mode** drop-down list, click the **On** option.
- In the **Radio Mode** drop-down list, click the **a/n** option for the AP3825, and click **a/n/ac** for the AP3865 and the 39xx series APs).
- In the **Channel Width** drop-down list, click **40 MHz** (for the AP3825 and for the AP3865 and 39xx series, click **80 MHz**).
- In the **Guard Interval** drop-down list, click **Short**.
- If only 802.11n devices are present, disable 11n protection and 40 MHz protection:
 - **Protection Mode** — Click **None**.
 - **Protection Type** — Click **CTS only** or **RTS CTS**.
- **Aggregate MSDUs** — Click **Enabled**.
- **Aggregate MPDU** — Click **Enabled**.
- **Aggregate MPDU Max Length** — Click **Enabled**.
- **Agg. MPDU Max # of Sub-frames** — Type **64**.
- **ADDBA Support** — Click **Enabled**.

6 From the top menu, click **VNS**.

7 In the left pane select **WLAN Services** and select the WLAN service to configure.

- 8 Click the **Privacy** tab. Some client devices do not use 802.11n mode if they are using WEP or TKIP for security. Do one of the following:
- Select **None**.
 - Select **WPA-PSK**, and then clear the **WPA v.1** option:
 - Select **WPA v.2**.
 - In the **Encryption** drop-down list, click **AES only**.

**Note**

To achieve the strongest encryption protection for your VNS, it is recommended that you use WPA v.2.

- 9 Click the **QoS** tab. From the QoS tab, you can select WMM and Flexible Client Access (FCA) to get better throughput.

**Note**

For FCA, go to **VNS > Global > Wireless QoS** and set the **Fairness Policy** to 100% Airtime.

- 10 In the **Wireless QoS** section, select the **WMM** option. Some 802.11n client devices remain at legacy rates.

NEW! Configuring IoT Applications

Configure IoT support from the **IoT** tab access point models AP391x

ExtremeWireless supports Real Time Location Systems (RTLS) on APs that offer integrated BLE/ 802.15.4 radios for connectivity to Internet of Things (IoT) sensors and devices. The AP must be BLE enabled.

ExtremeWireless supports the following applications. Each supported AP can be configured for one application at a time.

- **iBeacon** — AP is an Apple iBeacon. AP sends beacons in Apple iBeacon format.
- **iBeacon Scan** — AP scans for Apple iBeacons, filtering beacons based on configuration parameters and reports findings to an Application Server.
- **Eddystone-url Beacon** — AP sends a compressed URL in a beacon for automatic presentation of a website. Eddystone-url is supported by both iOS and Android 4.4 operating systems.
- **Eddystone-url Scan** — AP scans for Eddystone-url beacons, filtering beacons based on configuration parameters and reports findings to an Application Server.
- **Thread Gateway** — AP is a gateway router to the Thread Network. Thread is a mesh networking protocol based on IEEE 802.15.4 for IoT devices.

Related Links

[IoT iBeacon](#) on page 190

[IoT iBeacon Scan](#) on page 191

[Eddystone-url Beacon](#) on page 193

[Eddystone-url Scan](#) on page 195

[IoT Thread Gateway](#) on page 196

IoT iBeacon

iBeacon is Apple's technology standard that allows mobile apps to identify a beacon position in the physical world. It delivers content based on the identified location.

Extreme Wireless access point models AP391x support iBeacon.

Related Links

[Configuring AP as an iBeacon](#) on page 190

[IoT iBeacon Scan](#) on page 191

[Configuring IoT Applications](#) on page 189

[IoT Multi-Edit Configuration](#) on page 129

Configuring AP as an iBeacon

With the iBeacon application, configure a supported AP as an iBeacon in an IoT network. The following APs offer integrated BLE/802.15.4 radios: AP3912i, AP3915i/e, AP3916ic, AP3917i/e/k.

To configure iBeacon support from the **IoT** tab:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **IoT** tab, and select **IoT Admin**.
- 5 From the Application field, select **iBeacon**.

The screenshot shows the 'Edit AP' configuration window. At the top, there is a title bar 'Edit AP' with a help icon and a close icon. Below the title bar is a '<Back' link. The main area contains several tabs: 'AP Properties', 'WLAN Assignment', 'Radio 1', 'Radio 2', 'IoT', 'Static Configuration', and '802.1x'. The 'IoT' tab is selected and contains a sub-tab 'IoT Admin' which is checked. Under 'IoT Admin', there are several input fields: 'Application' is a dropdown menu set to 'iBeacon'; 'Advertise Interval' is a text box with '100' and 'ms' next to it; 'UUID' is a text box with '00000000-0000-0000-0000-000000000000'; 'Major' is a text box with '0'; and 'Minor' is a text box with '0'.

Figure 36: IoT Admin Tab iBeacon Application

- 6 Configure the following parameters:

Table 17: IoT iBeacon Application Settings

Field	Description
Application	Determines application type. Select iBeacon
Advertise Interval	The advertising interval for the beacon application. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).
UUID	Identifier used to differentiate a large group of related beacons. A company can have a network of beacons with the same UUID.
Major	Identifies <i>a subset of beacons</i> within the larger set. This value could represent a venue specific attribute, such as a specific store or wing in a building. Valid values are 0 to 65635.
Minor	Identifies <i>an individual beacon</i> . Used to more precisely pinpoint beacon location. This value complements the UUID and Major values to provide more granular identification of a specific location, such as a particular shelf, door-way, or item. Valid values are 0 to 65635.

Related Links

[IoT iBeacon](#) on page 190

[Configuring IoT Applications](#) on page 189

[IoT Multi-Edit Configuration](#) on page 129

IoT iBeacon Scan

With iBeacon Scan, an AP scans for beacons, filtering data based on configuration parameters and reports findings to an Application Server. ExtremeWireless forwards an iBeacon report as a JSON message to the customer's Application Server. The iBeacon report includes the following data:

- AP serial number
- The MAC address of the iBeacon tag
- The RSSI
- The signal strength of the iBeacon tag
- The UUID of the iBeacon tag including Major and Minor values.

The following filters can be applied at the AP to specify the message stream:

- UUID. The Global Unique Identifier. iBeacon messages with corresponding UUID are sent to the Application Server. All other UUID values are omitted.
- Minimum Received Signal Strength Indicator (RSSI). Transfers messages that meet the configured RSSI threshold. Messages received with an RSSI below the configured threshold are omitted.

Refer to the *Integration Guide* for details on the format of the iBeacon RTLS message.

The customer's Application Server handles the business logic and presentation of the IoT report. The Application Server:

- Calculates the distance between the BLE tag and the AP, based on the signal strength for the tag/radio channel
- Maps AP Serial Number to a physical location
- Tracks BLE tags.

From ExtremeWireless, configure iBeacon Scan parameters under AP configuration.

Related Links

- [Configuring iBeacon Scan](#) on page 192
- [IoT Multi-Edit Configuration](#) on page 129
- [Configuring IoT Applications](#) on page 189

Configuring iBeacon Scan

The following APs offer integrated BLE/802.15.4 radios: AP3912i , AP3915i/e, AP3916ic, AP3917i/e/k.

To configure iBeacon Scan support from the **IoT** tab:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **IoT** tab, and select **IoT Admin**.
- 5 From the Application field, select **iBeacon Scan**.

The screenshot shows the 'Edit AP' configuration window. At the top, there is a title bar 'Edit AP' with a help icon and a close icon. Below the title bar is a '<Back' link. The main content area has a tabbed interface with the following tabs: 'AP Properties', 'WLAN Assignment', 'Radio 1', 'Radio 2', 'IoT', 'Static Configuration', and '802.1x'. The 'IoT' tab is selected, and within it, the 'IoT Admin' sub-tab is active, indicated by a checkmark. The 'IoT Admin' section contains the following fields:

- Application:** A dropdown menu with 'iBeacon Scan' selected.
- Destination IP:** A text input field containing '0.0.0.0'.
- Destination Port:** A text input field containing '0'.
- Scan Interval:** A text input field containing '100' with 'ms' to its right.
- Scan Window:** A text input field containing '100' with 'ms' to its right.
- UUID:** A text input field containing '00000000-0000-0000-0000-000000000000'.
- Min RSSI:** A text input field containing '-100'.

At the bottom of the window, there are four buttons: 'Copy to Defaults', 'Reset to Defaults', 'Apply', and 'Close'.

Figure 37: iBeacon Scan Application

- 6 Configure the following parameters:

Table 18: iBeacon Scan Settings

Field	Description
Application	Determines application type. Select iBeacon Scan
Destination IP Address	IP address of the customer Application Server that receives the beacon report.
Destination Port	Destination Port on the customer Application Server that presents the beacon report.
Scan Interval	Determines how long to wait between scans. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).
Scan Window	Determines how long to scan per channel. Valid values are Min (100ms) and Max (10240ms). Value must be less than Scan Interval value. Default value is 100ms.
UUID	Identifier used to differentiate a large group of related beacons. A company can have a network of beacons with the same UUID. Used for filtering data. ExtremeWireless forwards data with matching UUID to the Application Server and filters out all other UUID data. If UUID configured value is all zeros, no filtering occurs.
Min RSSI	This is the signal strength required to include the packet in the BLE report. Valid values: -10 to -100. Default value is -100. Data from beacons with an RSSI that is less than the Min RSSI configured value is filtered out.

Related Links

[IoT iBeacon Scan](#) on page 191

[IoT Multi-Edit Configuration](#) on page 129

NEW! Eddystone-url Beacon

Eddystone-url is a Google technology standard that supports the physical web by providing a beacon-delivered URL that offers content based on the identified location. Eddystone-url is supported by both iOS and Android 4.4 operating systems.

An AP sends a beacon that includes a compressed URL. A mobile device app accepts the beacon, and the mobile user can access the URL that is provided in the beacon.

This technology automatically presents websites to mobile users at the AP location. Possible use cases include:

- Registration at a medical facility or school.
- Online payment at a parking garage.
- Detailed information about a museum exhibit.

The beacon format is defined by a Google specification. Both the URL and the Advertising Interval are configurable parameters on the AP.

Related Links

[Configuring AP as an Eddystone-url Beacon](#) on page 194

Configuring AP as an Eddystone-url Beacon

Configure an AP with integrated BLE radio as an Eddystone-url Beacon in an IoT network. The following APs offer integrated BLE/802.15.4 radios: AP3912i , AP3915i/e, AP3916ic, AP3917i/e/k.

To configure Eddystone-url Beacon support from the IoT tab:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **IoT** tab, and select **IoT Admin**.
- 5 From the Application field, select **Eddystone-url Beacon**.

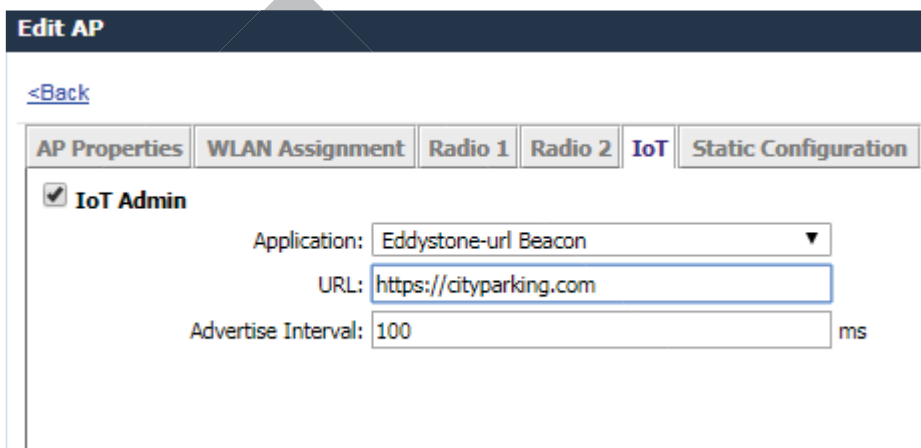


Figure 38: IoT Admin Tab Eddystone-url Beacon Application

- 6 Configure the following parameters:

Table 19: IoT Eddystone-url Beacon Application Settings

Field	Description
Application	Determines application type. Select Eddystone-url Beacon
URL	The URL that is included with the Eddystone-url beacon. The URL is limited to 17 characters. The 17 characters does not include the protocol, but it does include the domain name. A secure protocol (HTTPS address) is required. The URL is compressed, effectively allowing more than a 17-character input. See https://github.com/google/eddystone/tree/master/eddystone-url for the Eddystone-url compression rules to more accurately judge the length of your URL. If necessary, also find third-party URL Shortening Services available on the internet.
Advertise Interval	The advertising interval for the beacon application. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).

Related Links

- [Eddystone-url Beacon](#) on page 193
- [Configuring IoT Applications](#) on page 189
- [IoT Multi-Edit Configuration](#) on page 129

NEW! Eddystone-url Scan

BLE-enabled APs capture beacons and send them to a configured Application Server. Upon reception, the server application triggers possible actions such as updating statistics related to beacon location or communicating with a mobile device application.

An AP scans for beacons, filtering data based on configuration parameters and reports findings to an Application Server. ExtremeWireless forwards the report as a JSON message to the customer's Application Server. The report includes the following data:

- AP Serial Number
- The MAC address of the beacon tag
- Decoded URL
- Device transmission power
- The signal strength of the iBeacon tag

The following filters can be applied at the AP to specify the message stream:

- Minimum Received Signal Strength Indicator (RSSI). Transfers messages that meet the configured RSSI threshold. Messages received with an RSSI below the configured threshold are omitted.



Note

Only scanned frames with Eddystone-url format are supported. The UUID must be **0xFEAA**.

Refer to the *Integration Guide* for details on the format of the beacon RTLS message.

The customer's Application Server handles the business logic and presentation of the IoT report. The Application Server:

- Calculates the distance between the BLE tag and the AP, based on the signal strength for the tag/radio channel
- Maps AP Serial Number to a physical location
- Tracks BLE tags.

From ExtremeWireless, configure Eddystone-url Scan parameters under AP configuration.

Configuring Eddystone-url Scan

The following APs offer integrated BLE/802.15.4 radios: AP3912i, AP3915i/e, AP3916ic, AP3917i/e/k.

To configure Eddystone-url Scan support from the **IoT** tab:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **IoT** tab, and select **IoT Admin**.

- 5 From the Application field, select **Eddystone-url Scan**.

Edit AP

[<Back](#)

AP Properties | WLAN Assignment | Radio 1 | Radio 2 | **IoT** | Static Configuration

IoT Admin

Application: **Eddystone-url Scan** ▼

Destination IP: 188.42.0.16

Destination Port: 3

Scan Interval: 100 ms

Scan Window: 100 ms

Min RSSI: -100

Figure 39: Eddystone-url Scan Application

- 6 Configure the following parameters:

Table 20: Eddystone-url Scan Settings

Field	Description
Application	Determines application type. Select Eddystone URL Scan
Destination IP Address	IP address of the customer Application Server that receives the beacon report.
Destination Port	Destination Port on the customer Application Server that presents the beacon report.
Scan Interval	Determines how long to wait between scans. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).
Scan Window	Determines how long to scan per channel. Valid values are Min (100ms) and Max (10240ms). Value must be less than Scan Interval value. Default value is 100ms.
Min RSSI	This is the signal strength required to include the packet in the BLE report. Valid values: -10 to -100. Default value is -100. Data from beacons with an RSSI that is less than the Min RSSI configured value is filtered out.

Related Links

- [Eddystone-url Scan](#) on page 195
- [IoT Multi-Edit Configuration](#) on page 129
- [Configuring IoT Applications](#) on page 189

IoT Thread Gateway

The ExtremeWireless Thread Network solution makes use of a single infrastructure to combine a wireless network with an IoT sensor network, while integrating with an enterprise backbone network.

Each AP391x, with integrated BLE/802.15.4 radios, creates a separate Thread Network identified with a separate PAN ID. Sensors scan, find the AP Thread Network, and build a Mesh network with that AP serving as the border gateway router. The AP routes network traffic between its own Thread Network interface and the IoT interface.

To configure a Thread Network, do the following:

- Configure a VNS:
 - Create a new VNS.
 - Enable IPv6 multicast
- Assign a VLAN.



Note

The VLAN must have a Router with DHCPv6-PD — Thread Network supports IPv6 addressing only. If the DHCPv6 server provides global address, all sensors in the network receive the global address, and therefore, can be managed from the Cloud IPv6 network.

- Configure IoT Thread Gateway on an AP391x.
- Configure a WLANS with an IoT port enabled.
- Configure a whitelist that defines the allowed sensor nodes and joiner sensors for the Thread Network.



Note

If the whitelist is not configured, all sensors with password THREAD are accepted into the network.

Related Links

- [Configuring an AP as a Thread Gateway](#) on page 197
- [Advanced Thread Gateway Properties](#) on page 198
- [Managing an IoT Whitelist](#) on page 671
- [IoT Multi-Edit Configuration](#) on page 129

Configuring an AP as a Thread Gateway

To configure the Thread Network on each supported AP, take the following steps:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the AP row (not the check box) for an AP model that offers a BLE/802.15.4 radio.
The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **IoT** tab, and select **IoT Admin**.

- 5 From the Application field, select **Thread Gateway** and click **Advanced**.

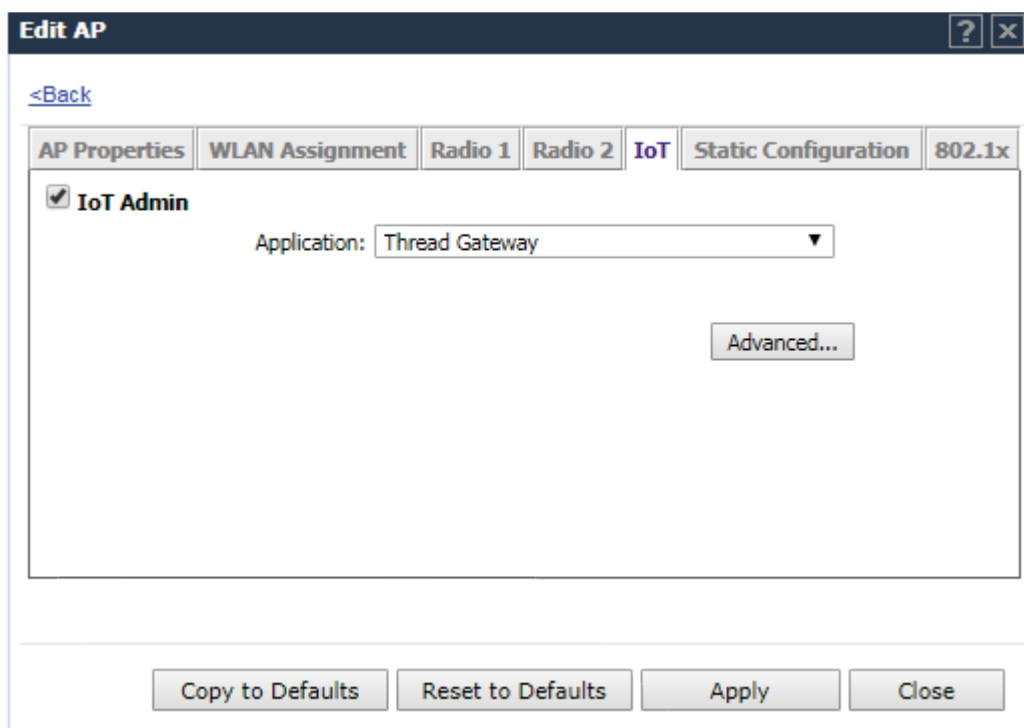


Figure 40: IoT Admin Tab Thread Gateway Application

The **Advanced** Thread Gateway parameters dialog displays.

Related Links

[Advanced Thread Gateway Properties](#) on page 198

[IoT Thread Gateway](#) on page 196

Advanced Thread Gateway Properties

Configure the following parameters on the selected AP. The AP serves as a border gateway router for its own Thread Network.

Advanced [?] [X]

Name: AP3915e-3915E000

Channel: 25

Short PAN ID: 4C4F

Extended PAN ID: 3928EAF6D914C90B

Master Key: 43A4ADB5279BB2DC601D3E7CB3115FF8

Close

Figure 41: IoT Thread Gateway Properties



Note

The configured Thread Gateway displays on the Active Clients report, indicating that the gateway is up and running.

Table 21: Thread Gateway Properties

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

Related Links

[Configuring an AP as a Thread Gateway](#) on page 197

[IoT Thread Gateway](#) on page 196

Setting Up the Wireless AP Using Static Configuration

Static configuration settings allow you to set up branch office support. These settings can be employed whenever required, and are not dependent on branch topology. In the branch office model, while the controller is at a central office, APs are installed in remote sites. The APs must be able to interact in both

the local site network and the central office network. When this is the case, a static configuration is recommended.

For initial configuration of a wireless AP to use a static IP address assignment:

- Allow the AP to first obtain an IP address using *DHCP*. By default, APs are configured to use the DHCP IP address configuration method.
- Allow the AP to connect to the controller using the DHCP assigned IP address.
- After the AP has successfully registered to the controller, use the **Static Configuration** tab to configure a static IP address for the AP, and then save the configuration.
- Once the static IP address has been configured on the AP, the AP can then be moved to its target location, if applicable.

Note

If a wireless AP with a statically configured IP address (without a statically configured Wireless Controller Search List) cannot register with the controller within the specified number of retries, the wireless AP uses SLP, DNS, and SLP multicast as a backup mechanism.

To set up a wireless AP using static configuration:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **Static Configuration** tab.
- 5 Configure the following parameters:
 - a Select a *VLAN (Virtual LAN)* setting for the AP.

Caution

Caution should be exercised when using this feature. For more information, see [Configuring VLAN Tags for Wireless APs](#) on page 203. If the Wireless AP VLAN is not configured properly (wrong tag), connecting to the AP may not be possible. To recover from this situation, you need to reset the AP to its factory default settings. For more information, see the Extreme Networks ExtremeWireless *Maintenance Guide*.

- b. Select a method of IP address assignment for the AP.

AP Properties
WLAN Assignment
Radio 1
Radio 2
Static Configuration

[Changing static configuration settings may cause the AP to reboot. Reboots caused by static configuration changes may make the AP unreachable from this EWC.]

VLAN Settings

Tagged - VLAN ID: (1-4094)
 Untagged

IP Address Assignment

Use DHCP
 Static Values

IP Address:

Netmask:

Gateway:

Ethernet Port

Ethernet Speed: ▼
Tunnel MTU:
 Ethernet Mode: ▼
 LACP

Wireless Controller Search List



Note

Client Port configuration is available for the AP3912. For more information, see [Assigning WLAN Services to Client Ports](#) on page 170.

Table 22: Static Configuration Properties

Field/Button	Description
VLAN Settings	
Tagged	Select if you want to assign this AP to a specific VLAN and type the value in the box.
Untagged	Select if you want this AP to be untagged. This option is selected by default.
VLAN ID	Enter a VLAN ID. Valid values are 2 to 4094
IP Address Assignment	

Table 22: Static Configuration Properties (continued)

Field/Button	Description
Use DHCP	Select to enable Dynamic Host Configuration Protocol (DHCP). This option is enabled by default.
Static Values	Select to specify the IP address of the AP.
IP Address	Type the IP address of the AP.
Netmask	Type the appropriate subnet mask to separate the network portion from the host portion of the address.
Gateway	Type the default gateway of the network.
Ethernet Port	
Ethernet Speed	If the AP has an Ethernet port, select values in the Ethernet Speed and Ethernet Mode drop down lists.
Ethernet Mode	If the AP has an Ethernet port, select values in the Ethernet Speed and Ethernet Mode drop down lists.
Tunnel MTU	Enter a static MTU value, from 600 to 1500, in the Tunnel MTU box. The maximum MTU can be increased to 1800 bytes by enabling Jumbo Frames support (for more information, see Setting Up the Data Ports on page 51). If the wireless software cannot discover the MTU size, it enforces the static MTU size. Set the MTU size to allow the source to reduce the packet size and avoid the need to fragment data packets in the tunnel.
LACP	Applies to the AP38xx and AP39xx only. Click to Enable Link Aggregation Control Protocol. This feature allows higher throughput by combining the two Ethernet ports. This feature is disabled by default.
Wireless Controller Search List	
Up	Select a controller and click the Up button to modify the order of the controllers. When an AP searches for a controller to register with, it begins with the first controller in the list.
Down	Select a controller and click the Up button to modify the order of the controllers. When an AP searches for a controller to register with, it begins with the first controller in the list.
Delete	Click to remove the controller from the list so that it can no longer control the AP.
Add	In the Add box, type the IP address of the controller that will control this AP then click the Add button to add the IP address is added to the list. Repeat this process to add the IP addresses of up to three controllers. This feature allows the AP to bypass the discovery process. If the Wireless Controller Search List box is not populated, the AP uses SLP unicast/multicast, DNS, or DHCP vendor option 43 to discover a controller. For the initial AP deployment, it is necessary to use one of the described options in Discovery and Registration on page 120.
Additional Buttons	
Copy to Defaults	To make this AP's configuration be the system's default AP settings, click Copy to Defaults. A pop-up dialog asking you to confirm the configuration change is displayed. To confirm resetting the system's default AP settings, click OK.

Table 22: Static Configuration Properties (continued)

Field/Button	Description
Reset to Defaults	If you have an AP that is already configured with its own settings, but would like the AP to be reset to use the system's default AP settings, use the Reset to Defaults feature
Apply	Click to save your changes.

Related Links

[AP Properties Tab Configuration](#) on page 159

[Assigning Wireless AP Radios to a VNS](#) on page 168

[Configuration Parameters for Radio Properties](#) on page 180

[Setting Up 802.1x Authentication for a Wireless AP](#) on page 203

Configuring VLAN Tags for Wireless APs**Caution**

Exercise caution while configuring a VLAN ID tag. If a VLAN tag is not configured properly, the connectivity between the controller and the AP will be lost.

To configure Wireless APs with a VLAN tag:

- 1 Connect the AP in the central office to the controller port (or to a network point) that does not require VLAN tagging.
- 2 From the top menu, click **AP**.
- 3 Click the **Static Configuration** tab.
- 4 In the **VLAN Settings** section, select **Tagged - VLAN ID**.
- 5 In the **Tagged - VLAN ID** text box, type the VLAN ID on which the AP operates.
- 6 To save your changes, click **Save**. The AP reboots and loses connection with the controller.
- 7 Log out from the controller.
- 8 Disconnect the AP from the central office network and move it to the target location.
- 9 Power up the AP. The AP connects to the controller.

If the AP does not connect to the controller, the AP was not configured properly. To recover from this situation, reset the AP to its factory default settings, and reconfigure the static IP address.

Setting Up 802.1x Authentication for a Wireless AP

802.1x is an authentication standard for wired and wireless LANs. The 802.1x standard can be used to authenticate access points to the LAN to which they are connected. 802.1x support provides security for network deployments where access points are placed in public spaces.

To successfully set up 802.1x authentication of a Wireless AP, the AP must be configured for 802.1x authentication before the AP is connected to a 802.1x enabled switch port.

**Caution**

If the switch port to which the AP is connected is not 802.1x enabled, the 802.1x authentication does not take effect.

802.1x authentication credentials can be updated at any time, whether or not the AP is connected with an active session. If the AP is connected, the new credentials are sent immediately. If the AP is not connected, the new credentials are delivered the next time the AP connects to the controller.

There are two main aspects to the 802.1x feature:

- Credential management — The controller and the AP are responsible for the requesting, creating, deleting, or invalidating the credentials used in the authentication process.
- Authentication — The AP is responsible for the actual execution of the EAP-TLS or PEAP protocol.

802.1x authentication can be configured on a per-AP basis. For example, 802.1x authentication can be applied to specific APs individually or with a multi-edit function.

The 802.1x authentication supports two authentication methods:

- PEAP (Protected Extensible Authentication Protocol)
 - Is the recommended 802.1x authentication method
 - Requires minimal configuration effort and provides equal authentication protection to EAP-TLS
 - Uses user ID and passwords for authentication of access points
- EAP-TLS
 - Requires more configuration effort
 - Requires the use of a third-party Certificate Authentication application
 - Uses certificates for authentication of access points
 - The controller can operate in either proxy mode or pass through mode.

Proxy mode — The controller generates the public and private key pair used in the certificate.

Pass through mode — The certificate and private key are created by the third-party Certificate Authentication application.

**Note**

Although a wireless AP can support using both PEAP and EAP-TLS credentials simultaneously, it is not recommended to do so. Instead, it is recommended that you use only one type of authentication and that you install the credentials for only that type of authentication on the wireless AP.

Related Links

[AP Properties Tab Configuration](#) on page 159

[Assigning Wireless AP Radios to a VNS](#) on page 168

[Configuration Parameters for Radio Properties](#) on page 180

[Setting Up the Wireless AP Using Static Configuration](#) on page 199

[Setting Up 802.1x Authentication for Wireless APs Using Managing Certificates](#) on page 209

Configuring 802.1x EAP-TLS Authentication

EAP-TLS authentication uses certificates for authentication. A third-party Certificate Authentication application is required to configure EAP-TLS authentication. Certificates can be overwritten with new ones at any time.

With EAP-TLS authentication, the controller can operate in the following modes:

- **Proxy Mode** on page 205
- **Pass Through Mode** on page 207



Note

When a wireless AP that is configured with 802.1x EAP-TLS authentication is connected to a controller, the AP begins submitting logs to the controller thirty days before the certificate expires to provide administrators with a warning of the impending expiry date.

Proxy Mode

In proxy mode, the controller generates the public and private key pair used in the certificate. You can specify the criteria used to create the Certificate Request. The Certificate Request that is generated by the controller is then used by the third-party Certificate Authentication application to create the certificate used for authentication of the Wireless AP. To successfully configure 802.1x authentication of a Wireless AP, the AP must first be configured for 802.1x authentication before the AP is deployed on a 802.1x enabled switch port.

To Configure 802.1x EAP-TLS Authentication in Proxy Mode:

- 1 From the top menu, click **AP**.
- 2 In the AP list, click the wireless AP (not the check box) for which you want to configure 802.1x EAP-TLS authentication.
- 3 Click the **802.1x** tab.
- 4 Click **Generate Certificate Signing Request**. The **Generate Certificate Signing Request** window is displayed.

Extreme™ **Generate Certificate Signing Request**
Connect Beyond the Network

Enter required information

Country name:

State or Province name:

Locality name (city):

Organization name:

Organizational Unit name:

Common name: MAC: 001B1B0B2508 ▼

Email address:

Key Size: 1024 bits ▼

- 5 Type the criteria to be used to create the certificate request. All fields are required:
 - **Country name** — The two-letter ISO abbreviation of the name of the country
 - **State or Province name** — The name of the State/Province
 - **Locality name (city)** — The name of the city
 - **Organization name** — The name of the organization
 - **Organizational Unit name** — The name of the unit within the organization
 - **Common name** — Click the value you want to assign as the common name of the wireless AP. (See [Table 23](#) on page 212 for credential parameters and values.)
 - **Email address** — The email address of the organization
- 6 Click **Generate Certificate Signing Request**. A certificate request file is generated (.csr file extension). The name of the file is the AP serial number. The **File Download** dialog is displayed.
- 7 Click **Save**. The **Save as** window is displayed.
- 8 Navigate to the location on your computer that you want to save the generated certificate request file, and then click **Save**.
- 9 In the third-party Certificate Authentication application, use the content of the generated certificate request file to generate the certificate file (.cer file extension).
- 10 On the **802.1x** tab, click **Browse**. The **Choose file** dialog is displayed.

- 11 Navigate to the location of the certificate file, and click **Open**. The name of the certificate file is displayed in the **X509 DER / PKCS#12 file** box.
- 12 To save your changes, click **Save**.

The 802.1x EAP-TLS (certificate and private key) authentication in proxy mode is assigned to the AP. The wireless AP can now be deployed to a 802.1x enabled switch port.

Pass Through Mode

In pass through mode, the certificate and private key are created by the third-party Certificate Authentication application. To successfully configure 802.1x authentication of a wireless AP, the AP must first be configured for 802.1x authentication before the AP is deployed on a 802.1x enabled switch port.

Before you configure 802.1x using EAP-TLS authentication in pass through mode, create a certificate using the third-party Certificate Authentication application and save the certificate file in PKCS #12 file format (.pfx file extension) on your system.

To Configure 802.1x EAP-TLS Authentication in Pass Through Mode:

- 1 From the top menu, click **AP**.
- 2 Click the appropriate wireless AP in the list (not the check box). The **AP** dashboard displays.
- 3 Click **Configure**. The **AP Properties** tab displays.
- 4 Click the **802.1x** tab.
- 5 Click **Browse**. The **Choose file** window is displayed.
- 6 Navigate to the location of the certificate file (.pfx) and click **Open**. The name of the certificate file is displayed in the **X509 DER / PKCS#12 file** box.
- 7 In the **Password** box, type the password that was used to protect the private key.



Note

The password that was used to protect the private key must be a maximum of 31 characters long.

- 8 To save your changes, click **Save**.

The 802.1x EAP-TLS authentication in pass through mode is assigned to the wireless AP. The AP can now be deployed to a 802.1x enabled switch port.

Viewing 802.1x Credentials

When 802.1x authentication is configured on a wireless AP, the light bulb icon on the **802.1x** tab for the configured AP is lit to indicate which 802.1x authentication method is used. A wireless AP can be configured to use both EAP-TLS and PEAP authentication methods. For example, when both EAP-TLS

and PEAP authentication methods are configured for the AP, both light bulb icons on the **802.1x** tab are lit.

Note



You can view only the 802.1x credentials of wireless APs that have an active session with the controller. If you attempt to view the credentials of a wireless AP that does not have an active session, the **AP Credentials** window displays the following message: Unable to query wireless AP: not connected.

To view current 802.1x credentials:

- 1 From the top menu, click **AP**.
- 2 In the AP list, click the wireless AP (not the check box) for which you want to view its current 802.1x credentials.
- 3 Select the **802.1x** tab.
- 4 In the **Current Credentials** section, click **Get Certificate details**.

The **Wireless AP Credentials** window is displayed.

The screenshot shows the 'Wireless AP Credentials' window with the following information:

Current credentials in use by Wireless AP	
PEAP	
Username:	0500008023050025
Password:	*****
EAP-TLS Certificate	
Serial number:	323EC87000000000015C
Expiry date:	Thursday, April 05th, 2012, 02:17:28 PM
Issued on:	Wednesday, April 06th, 2011, 02:17:28 PM
Issuer:	CN=restype, DC=com
Full subject distinguished name:	CN=Users, CN=AP1Credential, DC=com,
Subject alternative name:	Principal Name=ap_admin

Close

Deleting 802.1x Credentials



Caution

Exercise caution when deleting 802.1x credentials. For example, deleting 802.1x credentials may prevent the AP from being authenticated or cause it to lose its connection with the controller.

To delete current 802.1x credentials:

- 1 From the top menu, click **AP**.
- 2 In the AP list, click the wireless AP (not the check box) for which you want to view its current 802.1x credentials.
- 3 Select the **802.1x** tab.
- 4 Do the following:
 - To delete EAP-TLS credentials, click **Delete EAP-TLS** credentials.
 - To delete PEAP credentials, click **Delete PEAP** credentials.

The credentials are deleted and the AP settings are updated.



Note

If you attempt to delete the 802.1x credentials of a wireless AP that currently does not have an active session with the controller, the credentials are deleted only after the AP connects with the controller.

Setting Up 802.1x Authentication for Wireless APs Using Managing Certificates

In addition to configuring APs individually, you can also configure 802.1x authentication for multiple APs simultaneously by using the AP 802.1x Multi-edit feature.

When you use the AP 802.1x Multi-edit feature, you can choose to:

- Assign EAP-TLS authentication based on generated certificates to multiple APs by uploading a .pfx, .cer, or .zip file.
- Assign PEAP credentials to multiple APs based on a user name and password that you define


To configure 802.1x EAP-TLS Authentication in Proxy Mode using Multi-edit:

- 1 From the top menu, click **AP**.
The **AP** screen displays.

The screenshot shows the AP configuration interface. At the top, there is a navigation bar with tabs for Logs, Reports, Controller, AP (selected), VNS, and WIPS. Below the navigation bar is a search bar with the placeholder text "Search for AP Name, Site, Model ...". Underneath the search bar is a table listing APs with columns for Name, Model, Site, Location, SW Version, and Status. The table contains 10 rows of data. Below the table, there is a summary line: "Showing: 10 rows, Local: 5, Foreign: 5". At the bottom of the interface, there are five action buttons: "Actions", "Radio 1 Actions", "Radio 2 Actions", "New", and "Delete".

<input type="checkbox"/>	Name ▲	Model ◆	Site ◆	Location ◆	SW Version ◆	Status ◆
<input type="checkbox"/>	14300167085D0000	AP3825e			10.41.02.0002T	Foreign
<input type="checkbox"/>	1548Y-1007900000	AP3965i-ROW	s1		10.41.01.0075T	Local
<input type="checkbox"/>	3916	AP3916ic-ROW			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3715i	AP3715i			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3765i	AP3765i			10.41.02.0002T	Local
<input type="checkbox"/>	AP3912i-ROW-1	AP3912i-ROW			10.41.02.0002T	Foreign
<input type="checkbox"/>	AP3915	AP3915e-ROW			10.41.02.0002T	Local
<input type="checkbox"/>	Dual band	AP3765e			10.41.02.0002T	Local
<input type="checkbox"/>	W786	W786C-2IA-RJ45			10.41.02.0002T	Foreign
<input type="checkbox"/>	W788	W788C-2-RJ45			10.41.02.0002T	Local

Showing: 10 rows, Local: 5, Foreign: 5

- 2 In the **APs** list, select one or more APs to configure. To search for a specific AP, enter the AP in the search bar and click .
- 3 Click **Actions > Manage Certificates**
- 4 In the **Certificate Signing Request** section, type the following:
 - **Country name** — The two-letter ISO abbreviation of the name of the country
 - **State or Province name** — The name of the State/Province
 - **Locality name (city)** — The name of the city
 - **Organization name** — The name of the organization
 - **Organizational Unit name** — The name of the unit within the organization
 - **Common name** — Click the value you want to assign as the common name of the wireless AP (see [Table 23](#) on page 212 for credential parameters and values).
 - **Email address** — The email address of the organization
 - **Key Size** — If the email address key size is different from the default value shown, you can change it by selecting a new value from the drop down menu.

- 5 Click **Generate Certificates**. The **AP 802.1x Multi-edit progress** dialog is displayed, which provides the status of the configuration process. Once complete, the **File Download** dialog is displayed.
- 6 Click **Save**. The **Save as** window is displayed.
- 7 Navigate to the location on your computer that you want to save the generated **certificate_requests.tar** file, and then click **Save**.

The `certificate_requests.tar` file contains a certificate request (.csr) file for each AP.

- 8 Do one of the following:
 - For each certificate request, generate a certificate using the third-party Certificate Authentication application. This method produces a certificate for each wireless AP. Once complete, zip all the certificates files (.cer) into one .zip file.
 - Use one of the certificate requests and generate one certificate using the Certificate Authentication application. This method produces one certificate that can be applied to all APs.
- 9 In the **Bulk Certificate Upload** section, click **Browse**. The **Choose file** window is displayed.
- 10 Navigate to the location of the file (.zip or .cer), and then click **Open**. The name of the file is displayed in the **PFX, CER or ZIP Archive** box.
- 11 Click **Upload and Set certificates**.

Once complete, the **Settings updated** message is displayed in the footer of the Wireless Assistant.

The 802.1x EAP-TLS authentication configuration is assigned to the APs. The APs can now be deployed to 802.1x enabled switch ports.

Configuring 802.1x EAP-TLS Authentication in Pass Through Mode Using Multi-edit

When you configure 802.1x EAP-TLS authentication in pass through mode using Multi-edit, do one of the following:

- Generate a certificate for each AP using the third-party Certificate Authentication application. When generating the certificates:
 - Use the Common name value (either Name, Serial, or MAC) of the AP to name each generated certificate.
 - Use a common password for each generated certificate.
 - All .pfx files created by the third-party Certificate Authentication application must be zipped into one file.
- Generate one certificate, using the third-party Certificate Authentication application, to be applied to all APs. When generating the certificate, use the Common name value (either Name, Serial, or MAC) of the wireless AP to name the generated certificate.

The 802.1x PEAP authentication configuration is assigned to the APs. The APs can now be deployed to 802.1x enabled switch ports.

Managing Certificates

To configure certificates, take the following steps:

- 1 Certificate Signing Request
 - **Country name** — The two-letter ISO abbreviation of the name of the country
 - **State or Province name** — The name of the State/Province
 - **Locality name (city)** — The name of the city
 - **Organization name** — The name of the organization
 - **Organizational Unit name** — The name of the unit within the organization
 - **Common name** — Click the value you want to assign as the common name of the wireless AP (see [Table 23](#) on page 212 for credential parameters and values).
 - **Email address** — The email address of the organization
 - **Key Size** — If the email address key size is different from the default value shown, you can change it by selecting a new value from the drop down menu.
- 2 Click **Generate Certificates**. The **AP 802.1x Multi-edit progress** window is displayed, which provides the status of the configuration process. Once complete, the **File Download** dialog is displayed.
- 3 Click **Save**. The **Save as** window is displayed.
- 4 Navigate to the location on your computer that you want to save the generated **certificate_requests.tar** file, and then click **Save**.
The certificate_requests.tar file contains a certificate request (.csr) file for each AP.
- 5 Do one of the following:
 - For each certificate request, generate a certificate using the third-party Certificate Authentication application. This method produces a certificate for each wireless AP. Once complete, zip all the certificates files (.cer) into one .zip file.
 - Use one of the certificate requests and generate one certificate using the Certificate Authentication application. This method produces one certificate that can be applied to all APs.

Bulk Certificate Upload

- 6 Click **Browse**. The **Choose file** window is displayed.
- 7 Navigate to the location of the file (.zip or .cer), and then click **Open**. The name of the file is displayed in the **PFX, CER or ZIP Archive** box.
- 8 Click **Upload and Set certificates**. Once complete, the **Settings updated** message is displayed in the footer of the Wireless Assistant.
The 802.1x EAP-TLS authentication configuration is assigned to the APs. The APs can now be deployed to 802.1x enabled switch ports.

PEAP Authentication

PEAP authentication uses user ID and passwords for authentication. To successfully configure 802.1x authentication of a wireless AP, the AP must first be configured for 802.1x authentication before the AP is deployed on an 802.1x enabled switch port.

- 9 In the **Username** drop-down list, click the value you want to assign as the user name credential:
- 10 In the **Password** drop-down list, click the value you want to assign as the password credential.

Table 23: Credential Parameters

Parameter	Value
Name	The name of the wireless AP, which is assigned on the AP Properties tab. The AP name can be edited.
Serial	The serial number of the AP. This setting cannot be edited.

Table 23: Credential Parameters (continued)

Parameter	Value
MAC	The MAC address of the AP. The setting cannot be edited.
Other	Click to specify a custom value. A text box is displayed. In the text box, type the value you want to assign as the user name credential.

- 11 To save your changes, click **Save**.

The 802.1x PEAP authentication configuration is assigned to the AP. The AP can now be deployed to an 802.1x enabled switch port.

Related Links

[Setting Up 802.1x Authentication for Wireless APs Using Managing Certificates](#) on page 209

Configuring Co-Located APs in Load Balance Groups

You can configure APs that are co-located in an open area, such as a classroom, a conference hall, or an entrance lobby, to act as a load balance group. Load balancing distributes clients across the co-located APs that are members of the load balance group. The co-located APs should provide the same SSID, have Line-of-Sight (LoS) between each other, and be deployed on multiple channels with overlapping coverage.

Assign an AP's radio to the load balance group for the client distribution to occur. Load balancing occurs only among the assigned AP radios of the load balance group. Each radio can be assigned only to one load balance group. Multiple radios on the same AP do not have to be in the same load balance group. The radios that you assign to the load balance group must be on APs that are controlled by the same controller.

The load balance group uses one or more *WLAN* services for all APs assigned to the load balance group. You can configure two types of load balance groups:

- Client Balancing load group – performs load balancing based on the number of clients across all APs in the group and only for the WLANs assigned to the load group. This is different from load control in the Radio Preference group— load control APs make decisions in isolation from each other.
- Radio Preference load group – performs band preference steering and load control. Band preference steering is a mechanism to move 11a-capable clients to the 11a radio on the AP, relieving congestion on the 11g radio. No balancing is done between the 11a and 11g radios. Load control is disabled by default. A radio load group executes band preference steering and/or load control across the radios on each AP in the group. Each AP balances in isolation from the other APs, but all APs in the load group have the same configuration related to the band preference and load control.

Client balancing on the controller is AP-centric and requires no input from the client. The AP radios in the client balance group share information with secure (AES) messaging using multicast on the wired network. All APs in a client balance group must be in the same SIAPP cluster to ensure that each AP can reach all other APs in the client balance group over the wired subnet. If the APs in a client balance group are not in the same SIAPP cluster, client balancing happens independently within the subgroups defined by SIAPP clusters.

The benefits of configuring your co-located APs that are controlled by the same controller as a client balance group are the following:

- Resource sharing of the balanced AP
- Efficient use of the deployed 2.4 and 5 GHz channels
- Reduce client interference by distributing clients on different channels
- Scalable 802.11 deployment: if more clients need to be served in the area, additional APs can be deployed on a new channel

You can assign a maximum of 32 APs to a client balance group. [Table 24](#) lists the maximum number of load balance groups for each controller.

Table 24: Maximum Number of Load Balance Groups

ExtremeWireless Appliance	Number of load balance groups
C4110	32
C5110	64
C5210	64
C5215	64
C25	8
C35	8
V2110	64
V2110 (MS Hyper-V platform)	32

Currently, all APs support load balance groups.

To create a load balance group, see [Creating a Load Balance Group](#) on page 214.

Creating a Load Balance Group

To create a load balance group:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Load Groups**.
- 3 Click **New**. The **Add Load Group** window displays.

- 4 Enter a unique name for a load group ID, and select a Type from the drop-down menu and then click **Add**. The options are:
 - **Client Balancing** — load balancing based on the number of clients across all APs in the load balance group and only for the WLANs assigned to the group.
 - **Radio Preference** —band preference steering and load control on this load group.

If you are adding a Client Balancing load balancing group, the **Radio Assignment** tab becomes available.

Load Group ID: Type: *Client Balancing*

Radio Assignment
WLAN Assignment

Select AP radios: all radios ▼

	Radio 1(Available †)		Radio 2(Available †)	AP Name
<input checked="" type="checkbox"/>	a/n(7)	<input checked="" type="checkbox"/>	b/g(7)	0000000C29AC00AB
<input checked="" type="checkbox"/>	a/n(8)	<input checked="" type="checkbox"/>	b/g/n(7)	13310618085D0000
<input checked="" type="checkbox"/>	a/n/ac(8)	<input checked="" type="checkbox"/>	g/n(7)	2935
<input checked="" type="checkbox"/>	a/n(8)	<input checked="" type="checkbox"/>	b/g(8)	3705i
<input checked="" type="checkbox"/>	a/n/ac(8)	<input checked="" type="checkbox"/>	b/g/n(8)	3801i
<input checked="" type="checkbox"/>	a/n/ac(5)	<input checked="" type="checkbox"/>	g/n(4)	3805
<input checked="" type="checkbox"/>	a/n/ac(8)	<input checked="" type="checkbox"/>	g/n-strict(8)	3825i
<input checked="" type="checkbox"/>	a/n(8)	<input checked="" type="checkbox"/>	b/g/n(8)	3865e-1
<input checked="" type="checkbox"/>	a/n/ac(8)	<input checked="" type="checkbox"/>	g/n*(7)	39350000000000e1
<input checked="" type="checkbox"/>	a/n/ac(8)	<input checked="" type="checkbox"/>	g/n(7)	39350000000000i1
<input checked="" type="checkbox"/>	a/n(5)	<input checked="" type="checkbox"/>	g/n(6)	3935ssdfafafa111
<input checked="" type="checkbox"/>	a/n/ac*(8)	<input checked="" type="checkbox"/>	g/n*(7)	39650000000000e1
<input checked="" type="checkbox"/>	a/n/ac(8)	<input checked="" type="checkbox"/>	g/n(7)	39650000000000i1

† # of VNS available for load group WLAN Assignment for the radio.

* Radio assigned to another load balance group.

If you are adding a Radio Preference load balancing group, the **Radio Preference** tab becomes available.

Load Group ID: Type: *Radio Preference*

Radio Preference		WLAN Assignment										
Band Preference Enable: <input type="checkbox"/>		Load Control										
	<table border="1"> <thead> <tr> <th>Enable</th> <th>Max # of Clients</th> <th>Strict Limit</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input type="text" value="112"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="text" value="112"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Enable	Max # of Clients	Strict Limit	<input type="checkbox"/>	<input type="text" value="112"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="112"/>	<input type="checkbox"/>		
Enable	Max # of Clients	Strict Limit										
<input type="checkbox"/>	<input type="text" value="112"/>	<input type="checkbox"/>										
<input type="checkbox"/>	<input type="text" value="112"/>	<input type="checkbox"/>										
AP Assignment:												
AP Name(Radio 1 Available †, Radio 2 Available †)												
0000000C29AC00AB(7,7)		<input type="checkbox"/>										
13310618085D0000(8,7)		<input type="checkbox"/>										
2935(8,7)		<input type="checkbox"/>										
3705i(8,8)		<input type="checkbox"/>										
3805(5,4)		<input type="checkbox"/>										
3825i(8,8)		<input type="checkbox"/>										
3865e-1(8,8)		<input type="checkbox"/>										
3935000000000e1*(8,7)		<input type="checkbox"/>										

† # of VNS available for load group WLAN Assignment for the radio.
 * AP assigned to another load balance group.

The radios for both types of load groups can be assigned to a WLAN, on the **WLAN Assignment** tab.

Load Group ID: Type: *Radio Preference*

Radio Preference	WLAN Assignment
WLAN Name	
gggWLAN	<input type="checkbox"/>
h	<input type="checkbox"/>
httpsWLAN	<input type="checkbox"/>
Lab126-12-AAA	<input type="checkbox"/>
Lab126-12-Ext-CP	<input type="checkbox"/>
Lab126-12-Ext-CP-IA	<input type="checkbox"/>
Lab126-12-GuestP	<input type="checkbox"/>
Lab126-12-GuestSpl	<input type="checkbox"/>
Lab126-12-Int-CP	<input type="checkbox"/>
Lab126-12-Int-CP-bac	<input type="checkbox"/>
Lab126-12-MBA	<input type="checkbox"/>
o	<input type="checkbox"/>
v1WLAN	<input type="checkbox"/>
v1WLAND	<input type="checkbox"/>

You can filter the display of AP Groups. In the left pane, Expand **Client Balancing** to see only Client Balancing groups. Expand **Radio Preference** to see only Radio Preference groups.



Note

For more information about the fields on these screens, see [Configuration Parameters for AP Load Groups](#) on page 217.

Configuration Parameters for AP Load Groups

Table 25: AP Load Groups

Field/Button	Description
Load Group ID	Enter a unique name for the load group. You can create load groups with the same name on different controller; however, the groups are treated as separate groups according to the home controller where the group was originally created.
Type	The type of load group is displayed. Options include: <ul style="list-style-type: none"> Client Balancing - select to perform load balancing based on the number of clients across all APs in the load balance group and only for the <u>WLAN</u> Services assigned to the group. Radio Preference - select to perform band preference steering and enforce load control settings on this load group.

Table 25: AP Load Groups (continued)

Field/Button	Description
New	Click to create a new load group. The Add Load Group window.
Delete	Click to delete this load group.
Save	Click to save your changes.
Radio Assignment tab - Available for load groups assigned the Client Balancing type.	
Select AP Radios	<p>From the drop-down menu, select the AP radios that you want to assign to the load group. Options include:</p> <ul style="list-style-type: none"> • All radios • Radio 1 • Radio 2 • Clear all radios <p>You can assign a radio to only one load balance group. A radio that is assigned to another load balance group has an asterisk next to it. If you select a radio that has been assigned to another load balance group, the radio is reassigned to the new load balance group.</p> <p>Note: You can assign each radio of an AP to different load balance groups.</p>
Radio Preference tab - Available for load groups assigned the Radio Preference type	
Band Preference	<p>Select the Enable check box to enable band preference for this load group.</p> <p>You can apply band preference to a VNS assigned in the load group. Enabling band preference enables you to move an 11a-capable client to an 11a radio to relieve congestion on an 11g radio. A client is considered 11a capable if the AP receives requests on an 11a VNS that already belongs to a load group with band preference enabled. After you configure band preference, if a client tries to re-associate with an 11g radio, it is rejected if the AP determines that the client is 11a capable.</p>
Load Control	<p>Select the following parameters for each radio assigned to this load group:</p> <ul style="list-style-type: none"> • Enable: Select this check box to enable Radio Load Control (RLC) for individual radios (Radio1 and Radio2) associated with this Load Group. • Max. # of Clients: Enter the maximum number of clients for Radio 1 and Radio 2. The default limit is 60. The valid range is: 5 to 60. • Strict Limit: Select this check box to enable a strict limit on the number of clients allowed on a specific radio, based on the max # of clients allowed. Limits can be enforced separately for radio1 and radio 2.
AP Assignment	Select the APs on which you want to enforce the Band Preference and Load Control settings.

Table 25: AP Load Groups (continued)

Field/Button	Description
WLAN Assignment tab	
WLAN Name	Click the check box of the one or more WLAN services that you want to assign to all member radios of the load balance group. You can select up to the radio limit of eight VNSs. When you assign a radio to a load group, WLAN service assignment can be done only from the WLAN Assignment tab on the Wireless AP Load Groups screen. On all other WLAN Assignment tabs associated with the member AP radios, the radio check box associated with the member AP radios is grayed out. When you remove a radio from a load group, the load group's WLAN service remains assigned to the radio, but you can now assign a different WLAN service to the radio.

How Availability Mode Affects Load Balancing

All radios assigned to a load group must belong to APs that are all controlled by the same controller. Availability mode can be configured only from the home controller on which the load group was created. Load balancing continues to operate if member APs fail over to the foreign controller as long as the WLAN service assignment remains the same.

To ensure that load balancing works properly in availability mode, enable synchronization of the system configuration and the WLAN services used by the load group when you configure availability mode. If you do not enable synchronization, the radios on any AP that fails over may be removed from their assigned load groups. For more about availability mode, see [Configuring Availability Using the Availability Wizard](#) on page 539.

If you have not configured synchronization, in a failover situation you are able to change the load balance group's WLAN service assignment from the **VNS Configuration** screens and the **Wireless AP WLAN Assignment** screens on the foreign controller.

If you have configured synchronization, you cannot change the WLAN assignments from the foreign controller. If you have not configured synchronization, you must configure the foreign controller to ensure that all AP radios in the load balance group have the same WLAN services assigned before the AP fails over, as originally configured for the load group. If the WLAN services assigned do not match when an AP fails over, the affected AP radios are removed from the load group. If you change the WLAN services to match after the AP fails over, the AP radios still are not allowed to be in the load group. Reconnect the AP to the home controller to have the radios become part of the load group again.

Load Balance Group Statistics

You can view load balance group statistics through the **Active Wireless Load Groups** report. For more information, see [Viewing Load Balance Group Statistics](#) on page 631.

Configuring an AP Cluster

APs operating in both fit mode and standalone mode operate in a cluster setup. A cluster is a group of APs configured to communicate with each other. Mobile users (MU) can seamlessly roam between the APs participating in the cluster. Wireless APs extend basic cluster functions with the following enhancements:

- Client balancing across AP in the Load Group
- Client session synchronization between APs in the Site

APs operating on the same subnet with multicast and *IGMP (Internet Group Management Protocol)* snooping enabled can be formed into a cluster. You assign each AP a common, default cluster ID (shared secret).

An AP cluster can exist at any point in your network. Each cluster member periodically (every 30 seconds) sends a secure SIAPP (Siemens Inter-AP Protocol) multicast message to update other cluster members. The SIAPP message includes:

- The AP name
- The AP Ethernet MAC address
- The AP IP address
- The client count
- The base BSSIDs for both radios
- Client session information in a case when APs are members of a Site

Each AP caches locally-stored information about the other cluster members and maintains its own view of the cluster including the client session information in the Site.

To change an AP cluster's configuration:

- 1 From the top menu, click **AP**.

- In the left pane, click **Global Settings > AP Registration**.

Wireless AP Registration

Security Mode:

Allow all Wireless APs to connect

Allow only approved Wireless APs to connect

Discovery Timers:

Number of retries: (1 - 255)

Delay between retries: (1 - 10 seconds)

SSH Access:

Password:

Confirm password:

Secure Cluster:

Cluster Shared Secret:

Use Cluster Encryption

- In the **Secure Cluster** section, enter a cluster shared secret.
- Enable cluster encryption by clicking on the **User Cluster Encryption** check box. APs on which user cluster encryption is disabled cannot participate in the cluster.
- Enable or disable support for inter-AP roaming by clicking on the **Inter AP Roam** check box.
- Click **Save**.

Configuring an AP as a Guardian

Wireless access points that are configured as Guardians do not bridge traffic and instead devote all of the AP's resources to threat detection and countermeasures.

When an AP is **Approved as a Guardian**:

- The AP becomes a full time RADAR agent.
- The AP is added to a Guardian scan profile.
- The AP no longer provides services (WLAN service, load group, site) that were provided prior to the change.



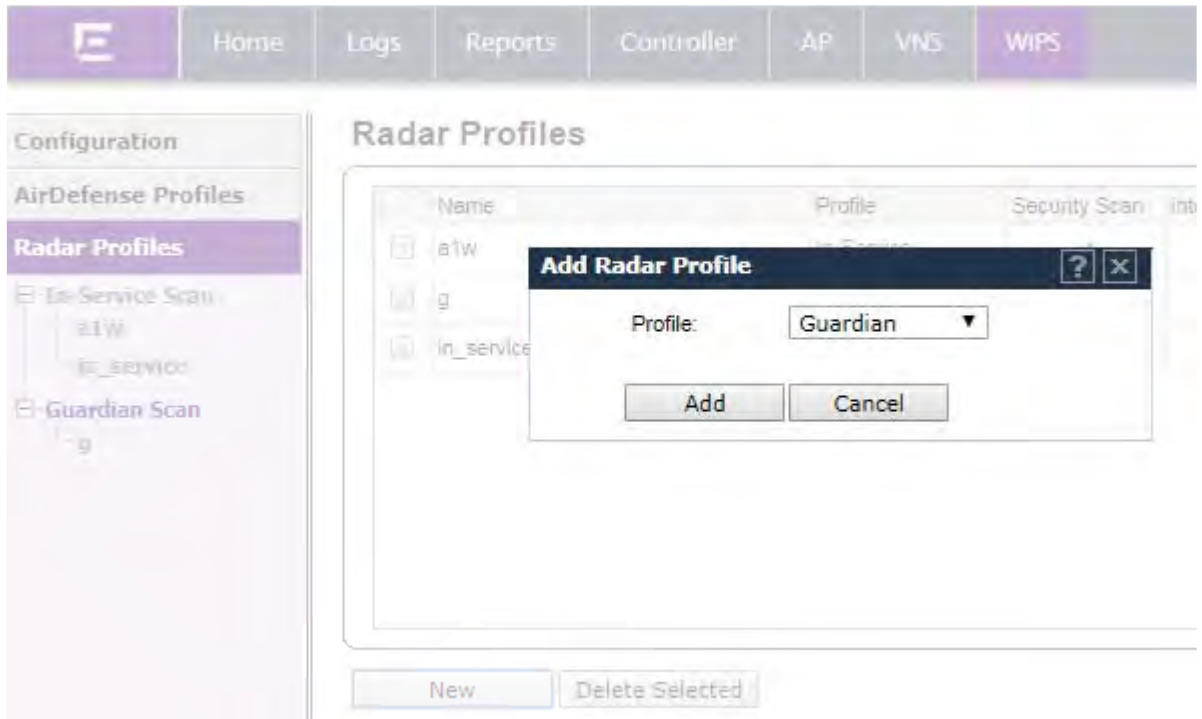
Note

Once an AP is assigned to a Guardian Scan Profile it will stop forwarding traffic on both radios.

To configure an AP as a Guardian Scan Profile:

- From the top menu, click **WIPS**.
- In the left pane, expand **Radar Profiles**.

- 3 In the left pane, expand **Guardian Scan** and select an AP from the list or click **New**.
- 4 In the **Add Scan Profile** dialog, select **Guardian** from the Profile drop-down.



- 5 Click **Add**.

For more information, see [Configuring a Guardian Scan Profile](#) on page 577.

Configuring a Captive Portal on an AP

ExtremeWireless offers a scalable captive portal solution on the AP that can be managed locally or through a Cloud solution. The distributed solution is available on ExtremeWireless AP38xx series and AP39xx series APs.

Firewall Friendly External Captive Portal (FFECP) on the AP for B@AP topologies is an extension to Firewall Friendly Captive Portal on the controller for tunneled (B@AC and routed) topologies.

You can configure the FFECP with full authentication using a URI and signature, or you can configure a RADIUS server, authenticating with a user name and password.

To configure an External Captive Portal on an AP, the following is required:

- The WLAN Service topology must be VLAN B@AP.
- You must configure specific policy rules that defines which traffic is allowed, which traffic is denied, and if using Rule-based Redirection, which traffic is redirected.
- The Captive Portal must be configured as External Firewall Friendly.



Note

ExtremeWireless supports a non-topology specific implementation. Extreme will register sub-domain “apcp.ezcloudx.com” and populate public/Extreme DNS server with DNS mapping of 1.1.1.1 for FQDN “apcp.ezcloudx.com”.

In [Figure 42](#), the default Access Control on the VLAN is Deny. Rules are created to allow the ECP URL, allow DNS and DHCP traffic, and to allow all outgoing MU traffic, and to redirect specific traffic.


VLAN & Class of Service		Policy Rules			
<input type="checkbox"/> Inherit filter rules from currently applied role 					
Rules					
Action	Name	Protocol	QoS	In	Out
Allow	host: ecp.com (group: Web Content Services)		None	Apply	Apply
Allow	0.0.0.0/0	Any	None	none	src
Allow	0.0.0.0/0:53 (DNS)	UDP	None	dest	src
Allow	0.0.0.0/0:67 (DHCP Server)	UDP	None	dest	src
Allow	0.0.0.0/0:68 (DHCP Client)	UDP	None	dest	src
Redirect	0.0.0.0/0:80 (HTTP)	TCP	None	dest	none
Redirect	0.0.0.0/0:8080 (HTTP)	TCP	None	dest	none
Redirect	0.0.0.0/0:443 (HTTPS)	TCP	None	dest	none

Figure 42: Example: Policy Rules for non-authenticated role

Related Links

[Configuring Firewall Friendly External Captive Portal on an AP](#) on page 223

[Controlling Network Access on the AP](#) on page 226

[Configuring Firewall Friendly External Captive Portal](#) on page 353

[Assigning RADIUS Servers for Authentication](#) on page 340

Configuring Firewall Friendly External Captive Portal on an AP

To configure a Firewall Friendly External Captive Portal (FFECP) on the AP, take the following steps:

- 1 If configuring Rule-based Redirection, verify that Rule-based Redirection is enabled. Go to **VNS > Global > Filtering Mode** and select **Enable Rule-Based Redirection**.

Rule-Based Redirection is enabled by default for new installations of ExtremeWireless v10.11 and later. When upgrading from an earlier version of ExtremeWireless, this option is cleared by default. You must enable Rule-Based Redirection from the **Filtering Mode** screen.



Note

The option to disable Rule-based Redirection is available for backward capability only.

Rule-based Redirection relies on policy rules that are defined for HTTP(S) redirection. Non-Rule-based Redirection automatically redirects an un-authenticated client to ECP when a deny action occurs on HTTP(S) traffic.



Note

You cannot configure Captive Portal Redirection using IPv6 classifiers. While you can http to IPv6 websites, you cannot apply Captive Portal redirection to http [s] over IPv6 .

- 2 Create a basic topology where the topology mode is **Bridge Traffic Locally at AP**. The topology can be tagged or untagged. For more information, see [Configuring a Basic Topology](#) on page 267 in the *User Guide*.

If using RADIUS authentication, FF-ECP on the AP can work with both local and central RADIUS authentication.

- 3 Create a role and define specific policy rules.

The role must be configured with the following parameters:

From the **VLAN & Class of Service** tab, select a default Access Control value for the role.

The screenshot shows the configuration page for a role named 'Allow_VLAN'. The page is titled 'Role: Allow_VLAN' and has a tab for 'VLAN & Class of Service'. The configuration is set for the 'Core' topology. The 'Role Name' is 'Allow_VLAN'. The 'Default Action' dropdown menu is open, showing options: 'None', 'No change', 'Allow' (which is highlighted in blue), 'Deny', and 'Containment VLAN'. The 'Default Class of Service' is set to 'Containment VLAN'. The 'Traffic Mirror' is set to 'None'.

Select from one of the following:

- None - No role defined
- No change - Default setting
- Allow - Packets contained to role's default action's VLAN/topology.
- Deny - Any packet not matching a rule in the Role is dropped.
- Containment VLAN - Any packet not matching a rule is sent to defined VLAN.

For B@AP traffic, only the FF ECP is supported as an external captive portal.

On the **Policy Rules** tab, enable **AP Filtering**.

Role: Allow_VLAN

VLAN & Class of Service	Policy Rules
<input type="checkbox"/> Inherit filter rules from currently applied role 	
Rules <input checked="" type="checkbox"/> AP Filtering <input type="checkbox"/> Custom AP Rules	

Configure specific policy filters.

- Allow *DHCP* and DNS traffic.
- Mobile user access to FF-ECP.
- Allow traffic towards mobile user.
- HTTP(S) redirection.



Note

ExtremeWireless supports a non-topology specific implementation. Extreme will register sub-domain “apcp.ezcloudx.com” and populate public/Extreme DNS server with DNS mapping of 1.1.1.1 for FQDN “apcp.ezcloudx.com”.

For more information, see [Configuring Rule-Based Redirection](#) on page 291 in the *User Guide*.

4 Configure a *WLAN* Service with the following parameter settings:

- Default Topology = **Bridged at AP**, tagged or untagged.
- Select an AP.
- Configure Privacy settings.
- Configure the Captive Portal to be **External Firewall Friendly**.
- (Optional) Configure RADIUS servers for RADIUS authentication. For more information, see [Assigning RADIUS Servers for Authentication](#) on page 340 in the *User Guide*.
- Configure the following parameters on the ECP:
 - The Identity and Shared Secret fields are required and must match the values used when you configured the captive portal.
 - When configuring the Allow policy for the ECP, the **IP/subnet** value specified on the **Filter Rule Definition** dialog must match the Redirection URL value specified on the FF-ECP **Configure** dialog.
 - Select the Vendor Specific Attributes (VSAs) for authentication. For more information, see [Vendor Specific Attributes](#) on page 344 in the *User Guide*.
 - Select an option for **Send Successful Login To**.

For FF-ECP local radius authentication:

- The AP must be in Site mode.
- Local RADIUS authentication is configured on at least one RADIUS server.
- The Signature option is unchecked.

5 Configure a VNS with the authenticated and non-authenticated policies.

Related Links

[Configuring a Basic Topology](#) on page 267

[Configuring Rule-Based Redirection](#) on page 291

- [Understanding the Filter Rule Definition Dialog](#) on page 302
- [Configuring a Basic WLAN Service](#) on page 319
- [Configuring WLAN Service Privacy](#) on page 330
- [Configuring Firewall Friendly External Captive Portal](#) on page 353
- [Assigning RADIUS Servers for Authentication](#) on page 340

Controlling Network Access on the AP

When Rule-based Redirection is disabled, denied HTTP(S) traffic from a non-authenticated client is automatically redirected to the External Captive Portal by the AP. To control network access after authentication, configure roles that have an Access Control of deny and specify that role under **Virtual Networks > General**.

To configure default roles that deny network access after authentication:

- 1 Go to **Virtual Networks** and select a VNS or click **New**.
- 2 Specify the default roles for Authenticated network traffic. In the **Authenticated** field under Default Roles, select a role or create a new role that has policy rules defined to deny access.

For more information, see [Understanding the Filter Rule Definition Dialog](#) on page 302

AP3916ic Integrated Camera Deployment

The AP3916ic features an integrated video camera, offering a single device for wireless access and security purposes. Video management is provided by the customer's Video Management System (VMS) integrated per ONVIF Profile S 2.4 compliance. The camera deployment process is as follows:

- 1 The AP3916ic is connected to the network and the controller discovers the camera IP address.

Per ONVIF specification, video management systems query network through WS-Discovery multicast (239.255.255.250). Allow multicast when configuring the default camera topology.

- Client IP = IP address of camera module
 - Device Type = Extreme Networks 2 MP Camera (EXTR2MP-CAM)
 - AP = AP camera module is 'associated' with Radio/Port = CAM
 - Packet/Byte counters = Indicate Camera Activity
- 2 Associate a WLAN B@AP or B@AC topology to the camera port.
 - 3 The camera requests a DHCP address.
 - 4 The EWC Active Clients Report lists the IP address of the camera. You can export the client IP address list to an XML file.

(Optional) The camera IP address can be detected by third-party tools, such as ONVIF Device Manager.



Note

ExtremeWireless manages the AP and camera firmware revision. After initial connection, the AP/camera may undergo a firmware upgrade. The upgrade process runs before the device becomes fully active on the network.

- 5 Based on the reported IP address of the camera, the user associates the camera to the video surveillance system.

For information about camera configuration settings, see [Accessing the Camera Web User Interface](#) on page 227.

Related Links

- [AP3916ic \(Integrated Camera\)](#) on page 104
- [Assigning WLAN Services to Client Ports](#) on page 170
- [Upgrading the Camera Image Manually](#) on page 237
- [Multicast Filtering](#) on page 281
- [AP3916ic-Camera Web User Interface](#) on page 227

Camera Direct Stream Subscription

If your video management system does not support ONVIF/IP camera discovery, subscribe directly using Real Time Streaming Protocol (RTSP). With direct stream, video is streamed through RTSP – H.264 or Motion JPEG (MJPEG):

- Stream 1:
 - Max Resolution: 1920x1080 (1080p)
 - RTSP URL: `rtsp://<Camera IP>:554/live/ch00_0`
- Stream 2:
 - Max Resolution: 640x360
 - RTSP URL: `rtsp://<Camera IP>:554/live/ch01_0`

AP3916ic-Camera Web User Interface

The AP3916ic is an 11ac Wave 2 AP with an integral security camera that lets you extend your Wireless LAN and provide simultaneous wireless service, BLE or 802.15.4 coverage and security in public spaces, such as classrooms and offices.

Extreme Networks offers a web-based user interface to customize and configure the camera.

Related Links

- [Accessing the Camera Web User Interface](#) on page 227
- [Camera UI Basic Functions](#) on page 228

Accessing the Camera Web User Interface

Take the following steps to access the AP3916ic Web User Interface:

- 1 Using your browser, navigate to the IP address of the camera.
Find the camera IP address on the AP dashboard of the AP3916ic. Go to the AP list and click on an AP3916ic.
- 2 Enter the camera IP address into your browser.
The web UI displays.



Figure 43: AP3916ic Web UI

- 3 Login with default credentials *admin/admin*. The credentials are case sensitive. Later, you can customize these credentials. See [User Management](#) on page 235.



Note

After the initial login, set a password in accordance with your IT policy regulations. Using default credentials is a security vulnerability for your network.

Related Links

- [AP3916ic \(Integrated Camera\)](#) on page 104
- [Camera UI Basic Functions](#) on page 228
- [AP3916ic Integrated Camera Deployment](#) on page 226
- [Camera Direct Stream Subscription](#) on page 227

Camera UI Basic Functions

Configure the AP3916ic camera using the web user interface. The AP3916ic web user interface is divided into the following tabs:

- [System](#) on page 229
- [Network](#) on page 231

- [Media](#) on page 232
- [User Management](#) on page 235

Related Links

[Accessing the Camera Web User Interface](#) on page 227

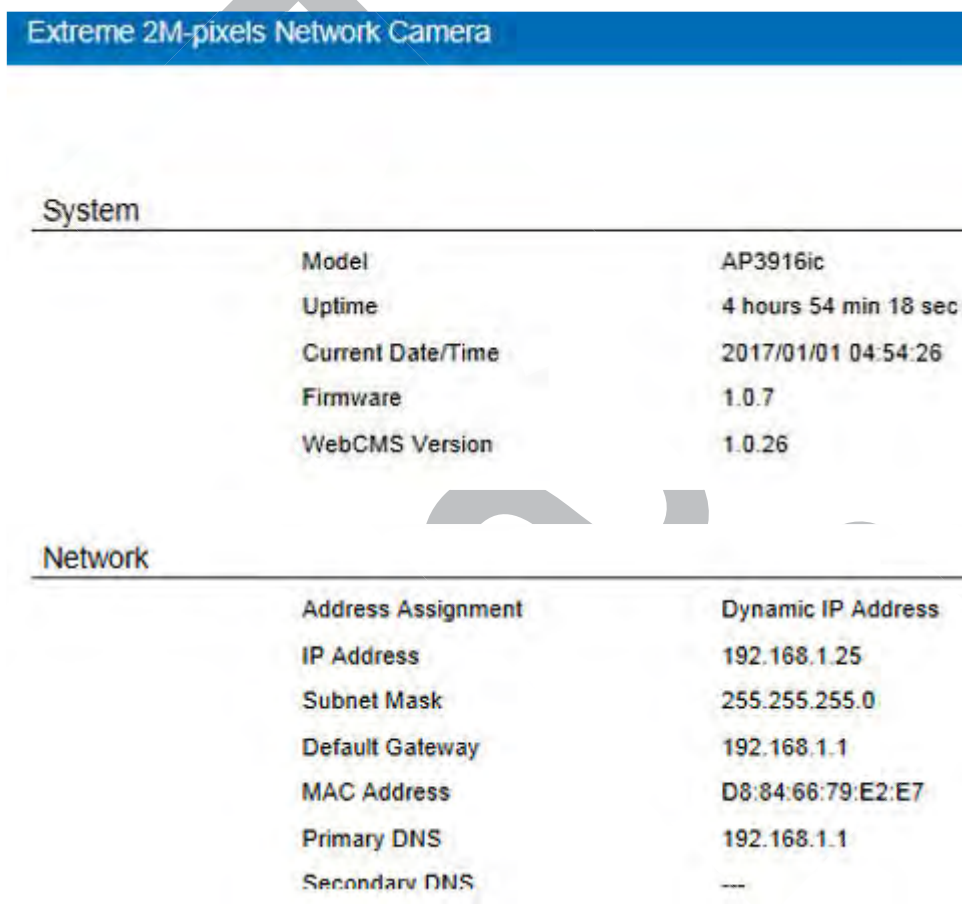
[AP3916ic \(Integrated Camera\)](#) on page 104

[Camera Direct Stream Subscription](#) on page 227

System

System settings for the AP3916ic camera:

- **Status** – Displays status information about the system, network, and video streams.



The screenshot shows the 'Extreme 2M-pixels Network Camera' status page. It is divided into two main sections: 'System' and 'Network'. The 'System' section lists details such as Model (AP3916ic), Uptime (4 hours 54 min 18 sec), Current Date/Time (2017/01/01 04:54:26), Firmware (1.0.7), and WebCMS Version (1.0.26). The 'Network' section lists details such as Address Assignment (Dynamic IP Address), IP Address (192.168.1.25), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.1), MAC Address (D8:84:66:79:E2:E7), Primary DNS (192.168.1.1), and Secondary DNS (---).

System	
Model	AP3916ic
Uptime	4 hours 54 min 18 sec
Current Date/Time	2017/01/01 04:54:26
Firmware	1.0.7
WebCMS Version	1.0.26

Network	
Address Assignment	Dynamic IP Address
IP Address	192.168.1.25
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MAC Address	D8:84:66:79:E2:E7
Primary DNS	192.168.1.1
Secondary DNS	---

Figure 44: Sample System and Network Status

Video		
Stream 1		
Resolution		1920 x 1080
Video Codec		H.264
Frame Rate		30 fps
Bit Rate Value		4 Mbps
Audio Codec		AAC
Stream 2		
Resolution		640 x 360
Video Codec		H.264
Frame Rate		15 fps
Bit Rate Value		256 Kbps
Audio Codec		AAC

Figure 45: Sample Video Status

- **Time** – Date/Time settings for the camera.

Extreme 2M-pixels Network Camera

Time Settings

Current Date/Time: 2017/01/01 05:05:18

Time Setup: Manual ▼

Date: 2017 ▼ / 3 ▼ / 5 ▼

Time: 20 ▼ : 33 ▼ : 45 ▼

Time Zone: (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼

Automatically adjust for daylight saving time changes.

Figure 46: Sample Manual Time settings

The screenshot shows the 'Time Settings' section of the camera's configuration interface. It includes the following fields and options:

- Current Date/Time:** 2017/01/01 05:09:24
- Time Setup:** A dropdown menu set to 'Synchronize with the NTP Server'.
- Time Zone:** A dropdown menu set to '(GMT-05:00)Eastern Time (US & Canada)'.
- NTP Time Server:** A text input field containing 'pool.ntp.org'.
- Automatically adjust for daylight saving time changes:** A checked checkbox.

Figure 47: Sample NTP Server Settings

- **Firmware** — Browse to the camera image (.dlf file) and apply the image. Camera firmware is distributed and managed from the controlling ExtremeWireless appliance. If GTAC Support determines that a specific firmware version is required on your device, the on-board firmware upload functionality can be used to install the image. GTAC will provide the necessary firmware (.dlf) file.
- **Backup** — Save camera settings to a backup file or restore settings from an existing backup file.

The screenshot shows the 'Backup Settings' section of the camera's configuration interface. It includes the following controls:

- Backup current settings to file:** A button labeled 'Backup'.
- Restore saved settings from file:** A text input field with a 'Browse...' button to its right, and an 'Upload' button below it.

Figure 48: Sample Backup /Restore Settings

- **Reset to Default/Reboot**
 - **Reset Camera Defaults** — Rest camera to factory default settings. Backup current settings before resetting to factory default settings.
 - **Reboot Camera** — Restarts the camera. The current camera settings are retained after a camera restart.

Network

Network settings for the AP3916ic camera.

- **IP Configuration** – Configure network settings for the camera port.



Note
Dynamic IP (DHCP) is the default network Mode.

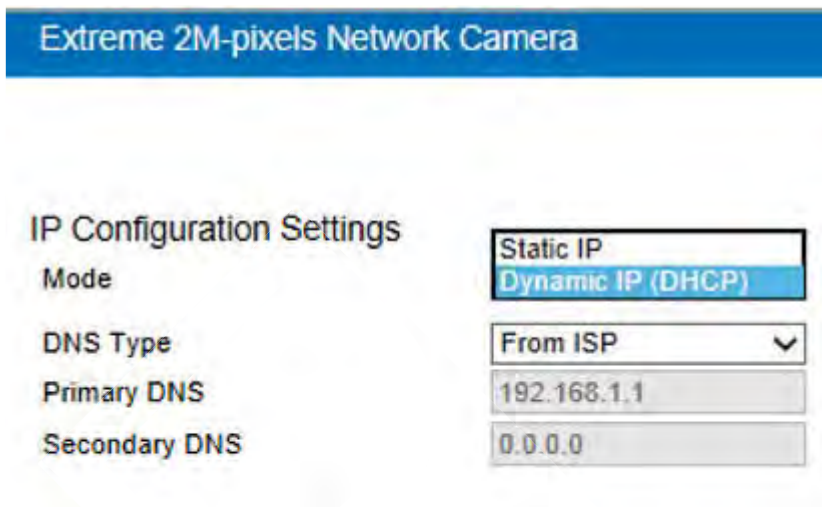


Figure 49: Sample IP Configuration Settings

- Universal Plug and Play (UPnP)



Figure 50: Sample Discovery Settings: UPnP

Media

Configure settings for: video, camera, advanced settings, privacy mask, and audio.

- **Video**

Extreme 2M-pixels Network Camera

Display overlay

Timestamp and Video Title (A-Z, 0-9, ., /, -)

Stream 1

Compression Format	H.264	▼
Resolution	1920 x 1080	▼
Max. Frame per Second	30 fps	▼
Bit Rate Encoding	Constant Bit Rate	▼
Bit Rate Value	4 Mbps	▼

Stream 2

Compression Format	H.264	▼
Resolution	640 x 360	▼
Max. Frame per Second	15 fps	▼
Bit Rate Encoding	Constant Bit Rate	▼
Bit Rate Value	256 Kbps	▼

Figure 51: Sample Video Configuration Settings

- **Camera**

The video feed assumes a ceiling mount default orientation. When installing the AP in any other orientation, adjust the video feed accordingly. For example, when the AP is installed as a desk-mount, the video Mirror/Flip setting should be **Flip**.

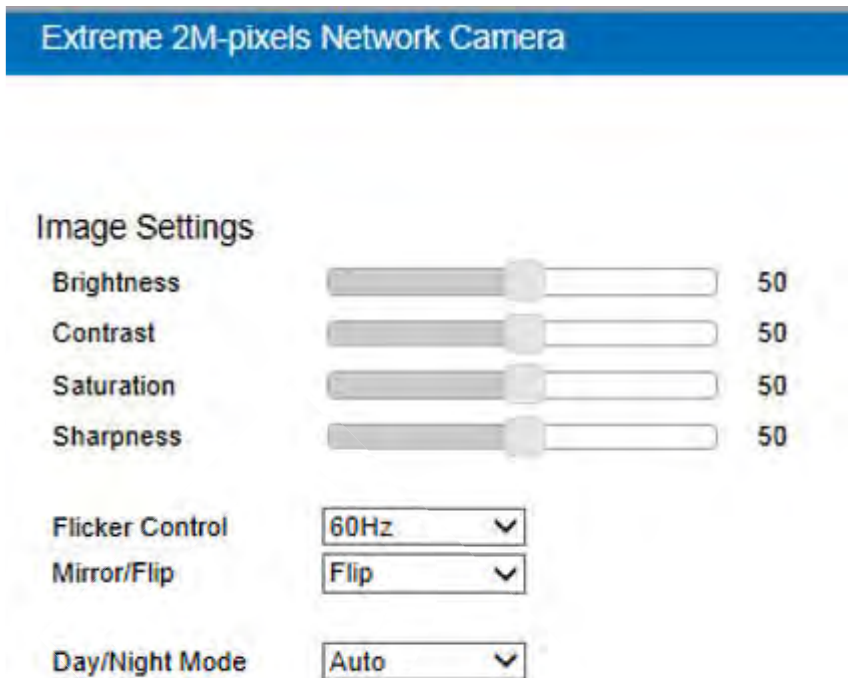


Figure 52: Sample Camera Settings

- Advanced

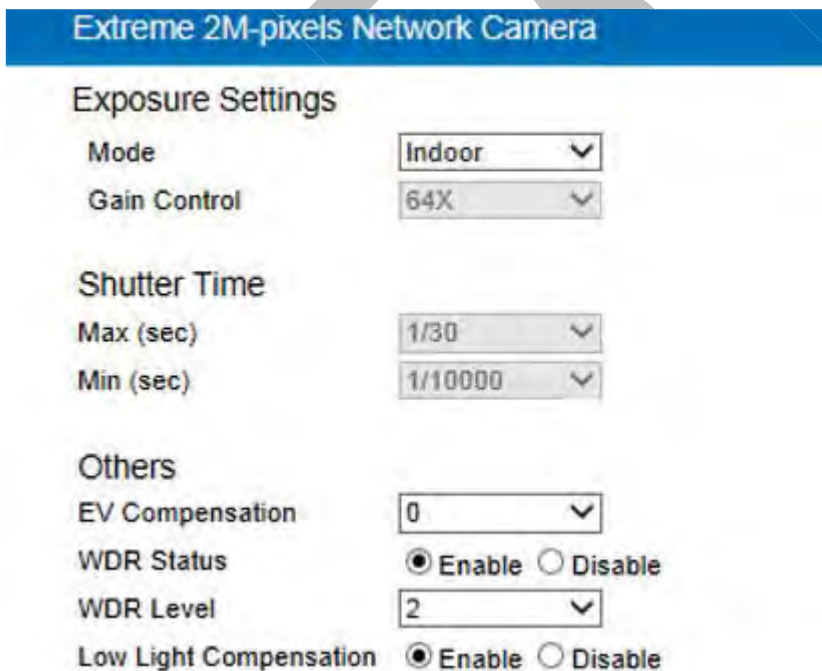


Figure 53: Sample Camera Advanced Settings

- Audio

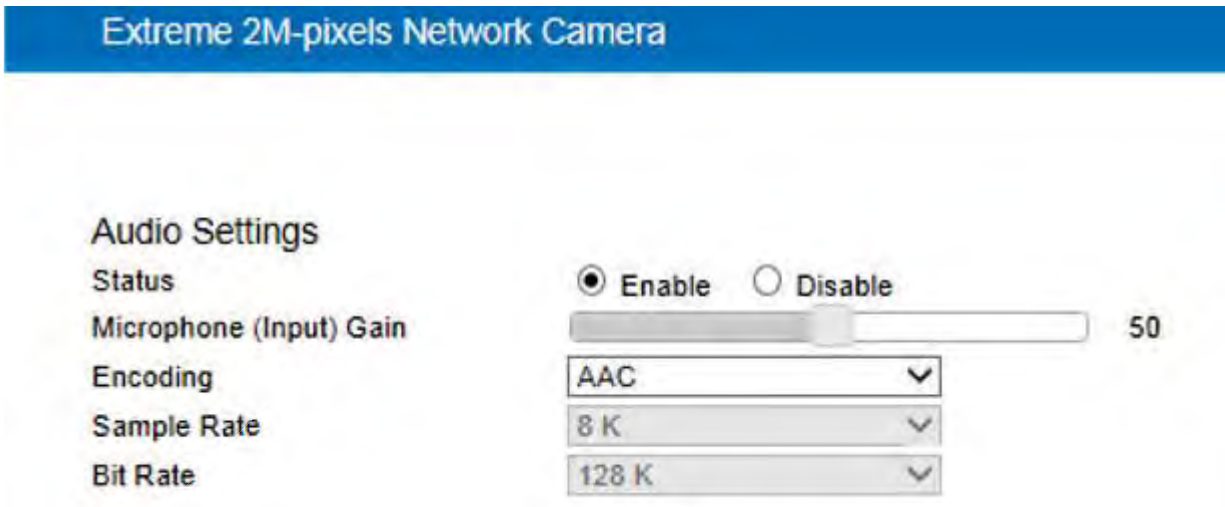


Figure 54: Sample Camera Audio Settings

User Management

Add and delete user accounts, change user settings, and change user password.

- **User List**



Figure 55: User Management Settings



Note

You cannot delete the Administrator account.

Performing AP Software Maintenance

When a new version of AP software becomes available, you can install it from the controller. You can configure each AP to upload the new software version either immediately, or the next time the AP connects to the controller. You can also set up a maintenance cycle for specific APs using the options

available on the AP Maintenance Cycle tab. Part of the AP boot sequence seeks and installs its software from the controller.



Warning

Never disconnect an AP from its power supply during a firmware upgrade. Disconnecting an AP from its power supply during a firmware upgrade may cause firmware corruption rendering the AP unusable.

You can modify most of the radio properties on an AP without requiring a reboot of the AP. During upgrade, the AP keeps a backup copy of its software image. When a software upgrade is sent to the AP, the upgrade becomes the AP's current image and the previous image becomes the backup. In the event of failure of the current image, the AP runs the backup image.

Maintaining the List of Current AP Software Images

To maintain the list of current wireless AP software images:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Maintenance**.

The following screen appears:

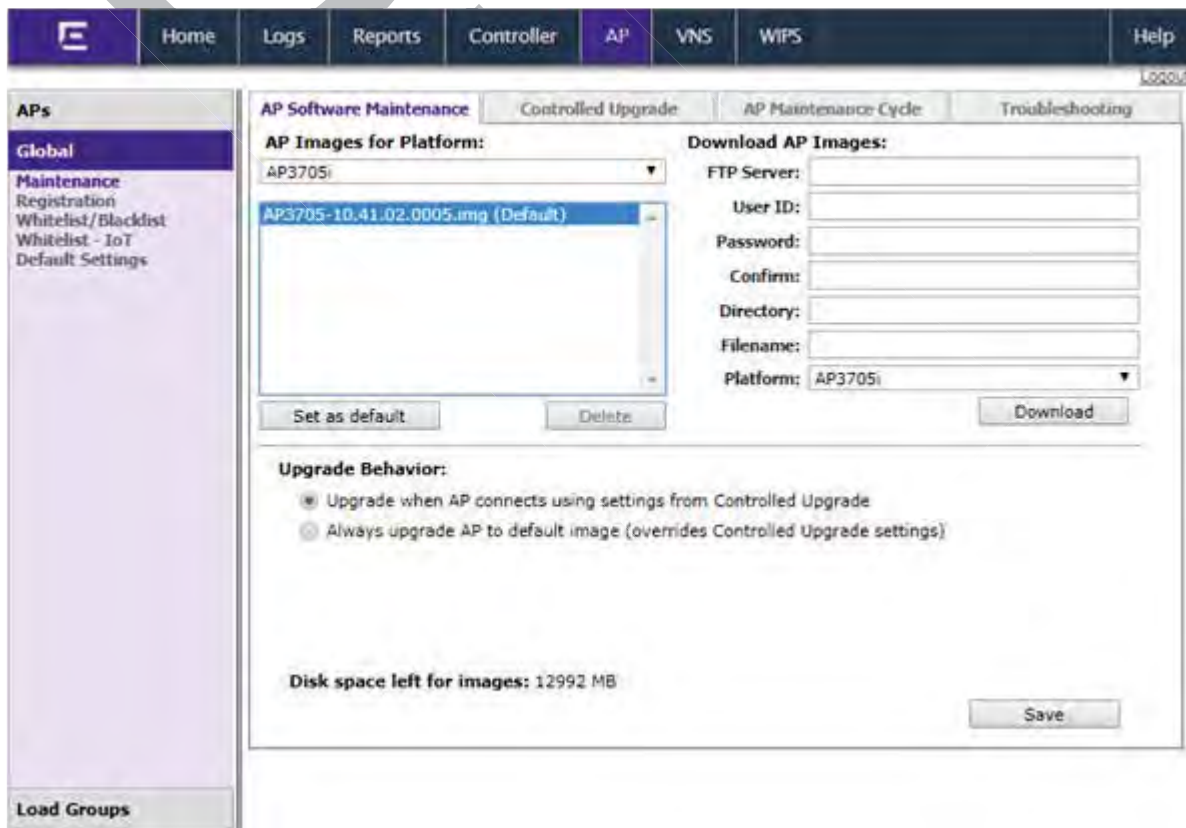


Figure 56: AP Software Maintenance

- 3 In the **AP Images for Platform** drop-down list, click the appropriate platform.
- 4 To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.

- 5 In the **Upgrade Behavior** section, select one of the following:
 - Upgrade when AP connects using settings from Controlled Upgrade — The **Controlled Upgrade** tab is displayed when you click **Save**. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.
 - Always upgrade AP to default image (overrides Controlled Upgrade settings) — Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.
- 6 To save your changes, click **Save**.

Related Links

[Upgrading the Camera Image Manually](#) on page 237

Upgrading the Camera Image Manually

The AP3916ic is an 11ac Wave 2 AP with an integral security camera that lets you extend your Wireless LAN and provide simultaneous wireless service, BLE or 802.15.4 coverage and security in public spaces, such as classrooms and offices.

The camera image (.dlf file) is distributed within the controller builds. The AP manages the camera image — camera images are automatically upgraded with the AP image upgrade when a new camera image is available.

You have the option to upgrade the camera image manually if necessary. To upgrade the AP3916ic camera image manually:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Maintenance**.
- 3 From the **AP Software Maintenance** tab, under **Download AP Images**:
 - a Provide the necessary information to download the camera image file.
 - b Select **AP3916-Camera** as the Platform.
 - c Click **Download**.
- 4 Under **Upgrade Behavior**, select **Upgrade when AP connects using settings from Controlled Upgrade**.

- Click **Save**.
- The Controlled Upgrade tab displays.

Figure 57: Manually Upgrading Camera Image

- Select the Controlled Upgrade tab.

Figure 58: Controlled Upgrade Tab

- Select AP Platform: **AP3916-camera**.
- Select the camera image file.
- Click **Camera Image Upgrade**.

Scheduling a Maintenance Cycle for Specific APs

To schedule a maintenance cycle for specific APs:

- 1 Go to **AP**.
- 2 In the left pane, click **Global Settings > Maintenance**.
- 3 Click the **AP Maintenance Cycle** tab.

The following screen appears:

- 4 Click the **Start At** box to display the **Choose Time** dialog.
- 5 Adjust the sliders for both Hour and Minute to set the time for the AP maintenance cycle, then click **Done**.
- 6 In the **Duration** drop-down, select the desired duration time (in hours).
- 7 Under **Recurrence**, select the desired frequency.
- 8 Under **Platforms**, select the AP(s) that are included in the maintenance cycle.
- 9 Click **Save**.

Deleting a Wireless AP Software Image

To delete a wireless AP software image:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Global > Maintenance**.
- 3 In the **AP Images for Platform** drop-down list, click the appropriate platform.
- 4 In the **AP Images** list, click the image you want to delete.

- 5 Click **Delete**. The image is deleted.

Downloading a new Wireless AP Software Image

To download a new wireless AP software image:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global Settings**, then **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
- 3 In the **Download AP Images** list, type the following:
 - **FTP Server** — The IP of the FTP server to retrieve the image file from.
 - **User ID** — The user ID for the controller to use when it attempts to log in to the FTP server.
 - **Password** — The corresponding password for the user ID.
 - **Confirm** — The corresponding password for the user ID to confirm it was typed correctly.
 - **Directory** — The directory on the server in which the image file to be retrieved is stored.
 - **Filename** — The name of the image file to retrieve.
 - **Platform** — The AP hardware type to which the image applies. There are several types of AP and they require different images.
- 4 Click **Download**. The new software image is downloaded.

Defining Parameters for a Controlled Software Upgrade

To define parameters for a wireless AP controlled software upgrade:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Maintenance**.
- 3 Under upgrade behavior, select **Upgrade when AP connects using settings from Controlled Upgrade**.
The **Controlled Upgrade** tab displays.

- 4 Click the **Controlled Upgrade** tab.

Logs
Reports
Controller
AP
VNS
WIPS

AP Software Maintenance
Controlled Upgrade
AP Maintenance Cycle
Troubleshooting

Step 1: Select AP Platform: AP3915

Step 2: Select an image to use: AP391x-10.41.02.0002T.img

Step 3: Apply the AP image from Step 2 to the selected APs below:

	Wireless APs	Current version	Upgrade to
<input type="checkbox"/>	1722D10010810000	10.41.02.0002T	

Select All
Deselect All
Apply AP image version

Step 4: Repeat Steps 1 - 3 as necessary

Step 5: Save this upgrade strategy for later, or upgrade the APs now:

Save for later
Upgrade Now
Upgrade without interrupting service



Note

The **Controlled Upgrade** tab is displayed only when the Upgrade Behavior is set to **Upgrade when AP connects using settings from Controlled Upgrade** on the **AP Software Maintenance** tab.

- 5 In the **Select AP Platform** drop-down list, click the type of AP you want to upgrade.
- 6 In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.
- 7 In the list of registered **Wireless APs**, select the check box for each AP to be upgraded with the selected software image.
- 8 Click **Apply AP image version**. The selected software image is displayed in the **Upgrade To** column of the list.
- 9 To save the software upgrade strategy to be run later, click **Save for later**.

- 10 To run the software upgrade immediately, click **Upgrade Now**. The selected AP reboots, and the new software version is loaded.

**Note**

The Always upgrade AP to default image check box on the **AP Software Maintenance** tab overrides the Controlled Upgrade settings.

- 11 To upgrade without interrupting service, click **Upgrade without interrupting service**. If you click this option while the upgrade scheduler is running, the schedule is interrupted, and the current upgrade cycle calculates a new schedule that includes APs that weren't upgraded.

Understanding the ExtremeWireless LED Status

When you power on and boot an AP, you can follow its progress through the registration process by observing the LED sequence as described in the following sections:

- [39xx Series Wireless APs](#)
- [38xx Series Wireless APs](#) on page 251
- [37xx Series Wireless APs](#) on page 255

After you power on and boot the AP for the first time, you can configure LED behavior as described in [Configuring Wireless AP LED Behavior](#) on page 259.

39xx Series Wireless APs

The following AP39xx model access points are supported by ExtremeWireless:

- AP3917i/e
- AP3916i/e
- AP3915i/e
- AP3912i/e
- AP3935i/e
- AP3965i/e