



ExtremeWireless™ User Guide

Release V10.21.03



Copyright © 2017 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

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

Chapter 1: About This Guide.....	8
Intended Audience.....	8
How to Use This Guide.....	8
Safety Information.....	10
Sicherheitshinweise.....	11
Consignes De Sécurité.....	12
Text Conventions.....	13
Providing Feedback to Us.....	13
Getting Help.....	14
Related Publications.....	14
Chapter 2: Overview of the ExtremeWireless Solution.....	16
Introduction.....	16
Conventional Wireless LANs.....	17
Elements of the ExtremeWireless Solution.....	17
ExtremeWireless and Your Network.....	21
ExtremeWireless Appliance Product Family.....	31
Chapter 3: Configuring the ExtremeWireless Appliance.....	33
System Configuration Overview.....	33
Logging on to the ExtremeWireless Appliance.....	35
Wireless Assistant Home Screen.....	36
Working with the Basic Installation Wizard.....	41
Configuring the ExtremeWireless Appliance for the First Time.....	47
Using a Third-party Location-based Solution.....	93
Additional Ongoing Operations of the System.....	97
Chapter 4: Configuring the ExtremeWireless APs.....	98
Wireless AP Overview.....	98
Discovery and Registration.....	119
Wireless AP Default Configuration.....	130
Configuring Wireless AP Properties.....	147
Assigning Wireless AP Radios to a VNS.....	156
Configuring Wireless AP Radio Properties.....	162
Setting Up the Wireless AP Using Static Configuration.....	173
Setting Up 802.1x Authentication for a Wireless AP.....	177
Configuring Co-Located APs in Load Balance Groups.....	187
Configuring an AP Cluster.....	194
Configuring an AP as a Guardian.....	195
Configuring a Captive Portal on an AP.....	196
Performing AP Software Maintenance.....	200
Understanding the ExtremeWireless LED Status.....	205
Chapter 5: Configuring Topologies.....	219
Topology Overview.....	219
Configuring the Admin Port.....	220
Configuring a Basic Data Port Topology.....	223
Creating a Topology Group.....	226
Edit or Delete a Topology Group.....	227

Enabling Management Traffic.....	228
Layer 3 Configuration.....	228
Exception Filtering.....	234
Multicast Filtering.....	237
Chapter 6: Configuring Roles.....	240
Roles Overview.....	240
Configuring Default VLAN and Class of Service for a Role.....	240
Policy Rules.....	243
Chapter 7: Configuring WLAN Services.....	273
WLAN Services Overview.....	273
Third-party AP WLAN Service Type.....	274
Configuring a Basic WLAN Service.....	274
Configuring Privacy.....	282
Configuring Accounting and Authentication.....	289
Configuring QoS Modes.....	323
Configuring Hotspots.....	329
Chapter 8: Configuring a VNS.....	343
Configuring a VNS.....	343
VNS Global Settings.....	345
Methods for Configuring a VNS.....	373
Manually Creating a VNS.....	374
Creating a VNS Using the Wizard.....	376
Enabling and Disabling a VNS.....	437
Renaming a VNS.....	438
Deleting a VNS.....	438
Chapter 9: Configuring Classes of Service.....	439
Classes of Service Overview.....	439
Configuring Classes of Service.....	439
CoS Rule Classification.....	442
Priority and ToS/DSCP Marking.....	443
Rate Limiting.....	444
Chapter 10: Configuring Sites.....	446
VNS Sites Overview.....	446
Configuring Sites.....	446
Recommended Deployment Guidelines.....	447
Radius Configuration.....	451
Selecting AP Assignments.....	452
Selecting WLAN Assignments.....	453
Chapter 11: Working with a Mesh Network.....	455
About Mesh.....	455
Simple Mesh Configuration.....	455
Wireless Repeater Configuration.....	456
Wireless Bridge Configuration.....	457
Examples of Deployment.....	458
Mesh WLAN Services.....	458
Key Features of Mesh.....	462
Deploying the Mesh System.....	464

Changing the Pre-shared Key in a Mesh WLAN Service.....	470
Chapter 12: Working with a Wireless Distribution System.....	471
About WDS.....	471
Simple WDS Configuration.....	471
Wireless Repeater Configuration.....	472
Wireless Bridge Configuration.....	473
Examples of Deployment.....	474
WDS WLAN Services.....	474
Key Features of WDS.....	478
Deploying the WDS System.....	481
Changing the Pre-shared Key in a WDS WLAN Service.....	489
Chapter 13: Availability and Session Availability.....	490
Availability.....	490
Session Availability.....	498
Viewing SLP Activity.....	507
Chapter 14: Configuring Mobility.....	509
Mobility Overview.....	509
Mobility Domain Topologies.....	510
Configuring a Mobility Domain.....	512
Chapter 15: Working with Third-party APs.....	515
Defining Authentication by Captive Portal for the Third-party AP WLAN Service.....	515
Defining the Third-party APs List.....	515
Defining Policy Rules for the Third-party APs.....	515
Chapter 16: Working with ExtremeWireless Radar.....	517
Radar Overview.....	517
Radar Components.....	517
Radar License Requirements.....	519
Radar Scan Profiles.....	519
Enabling the Analysis Engine.....	520
Viewing Existing Scan Profiles.....	521
Adding a New Scan Profile.....	522
Configuring an In-Service Scan Profile.....	523
Configuring a Guardian Scan Profile.....	528
Maintaining the Radar List of APs.....	533
Working with Radar Reports.....	542
Chapter 17: Working with Location Engine.....	553
Location Engine Overview.....	553
Location Engine on the Controller.....	555
Deploying APs for Location Aware Services.....	556
Configuring the Location Engine.....	557
Chapter 18: Working with Reports and Statistics.....	566
Application Visibility and Device ID.....	566
Viewing AP Reports and Statistics.....	572
Viewing All Clients.....	587
Viewing Role Filter Statistics.....	591
Viewing Topology Reports.....	593

Viewing Mobility Reports.....	596
Viewing Controller Status Information.....	601
Viewing Routing Protocol Reports.....	604
Viewing RADIUS Reports.....	608
Call Detail Records (CDRs).....	610
Chapter 19: Performing System Administration.....	615
Performing Wireless AP Client Management.....	615
Defining Wireless Assistant Administrators and Login Groups.....	618
Chapter 20: Logs, Traces, Audits and DHCP Messages.....	621
ExtremeWireless Appliance Messages.....	621
Working with Logs.....	621
Viewing Wireless AP Traces.....	629
Viewing Audit Messages.....	630
Viewing the DHCP Messages.....	630
Viewing the NTP Messages.....	631
Viewing Software Upgrade Messages.....	632
Viewing Configuration Restore/Import Messages.....	633
Chapter 21: Working with GuestPortal Administration.....	635
About GuestPortals.....	635
Adding New Guest Accounts.....	635
Enabling or Disabling Guest Accounts.....	638
Editing Guest Accounts.....	639
Removing Guest Accounts.....	639
Importing and Exporting a Guest File.....	640
Viewing and Printing a GuestPortal Account Ticket.....	643
Working with the Guest Portal Ticket Page.....	645
Configuring Guest Password Patterns.....	646
Configuring Web Session Timeouts.....	649
Appendix A: Regulatory Information.....	650
ExtremeWireless APs 37XX , 38XX, and 39XX.....	650
Appendix B: Default GuestPortal Ticket Page.....	651
Example Ticket Page.....	651
Appendix C: Glossary.....	654
A.....	654
B.....	656
C.....	658
D.....	661
E.....	664
F.....	667
G.....	669
H.....	669
I.....	670
J.....	673
L.....	673
M.....	675
N.....	678
O.....	679

P.....681
Q.....684
R.....684
S.....686
T.....690
U.....692
V.....692
W.....694
X.....695



1 About This Guide

[Intended Audience](#)
[How to Use This Guide](#)
[Safety Information](#)
[Sicherheitshinweise](#)
[Consignes De Sécurité](#)
[Text Conventions](#)
[Providing Feedback to Us](#)
[Getting Help](#)
[Related Publications](#)

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.

Intended Audience

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

This preface provides an overview of this guide and a brief summary of each chapter, defines the conventions used in this document; and instructs how to obtain technical support from Extreme Networks.

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 16
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 33
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 98
An overview of topologies and provides detailed information about how to configure them.	Configuring Topologies on page 219

For...	Refer to...
An overview of roles and provides detailed information about how to configure them.	Configuring Roles on page 240
An overview of WLAN services and provides detailed information about how to configure them.	Configuring WLAN Services on page 273
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 343
Information about configuring 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 439
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 446
An overview of Mesh networks and provides detailed information about how to create a Mesh network.	Working with a Mesh Network on page 455
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 471
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 490
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 509
Information on how to use the ExtremeWireless AP features with third-party wireless access points.	Working with Third-party APs on page 515
Information on the security tool that scans for, detects, provides countermeasures, and reports on rogue APs.	Working with ExtremeWireless Radar on page 517
Information on the various reports and displays available in the system.	Working with Reports and Statistics on page 566
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 615
Information on how to view and interpret the logs, traces, audits and messages.	Logs, Traces, Audits and DHCP Messages on page 621
Information on how to configure GuestPortal accounts.	Working with GuestPortal Administration on page 635
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 on page 654
Regulatory information for the ExtremeWireless Appliances and the ExtremeWireless APs.	Regulatory Information on page 650
The default GuestPortal ticket page source code.	Default GuestPortal Ticket Page on page 651

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).

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.
	New	This command or section is new for this release.

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.

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:

- **Global Technical Assistance Center (GTAC) 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.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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 Return Material Authorization (RMA) numbers

Related Publications

ExtremeWireless and ExtremeWireless AP documentation can be found on Extreme Documentation page at: <http://documentation.extremenetworks.com>

Extreme recommends the following guides for users of ExtremeWireless products:

- *ExtremeWireless AP3912i Installation Guide*
- *ExtremeWireless AP3965i & AP3965e Installation Guide*
- *ExtremeWireless AP3935i & AP3935e Installation Guide*
- *ExtremeWireless AP3825i & AP3825e Installation Guide*
- *ExtremeWireless AP3805i FCC/ROW Installation Guide*
- *ExtremeWireless AP3801i Quick Reference Guide*
- *ExtremeWireless Appliance C5210 Quick Reference*
- *ExtremeWireless Appliance C5110 Quick Reference*
- *ExtremeWireless Appliance C4110 Quick Reference*
- *ExtremeWireless Appliance C25 Quick Reference*
- *ExtremeWireless Appliance C35 Quick Reference*

- [*ExtremeWireless CLI Reference Guide*](#)
- [*ExtremeWireless End User License Agreements*](#)
- [*ExtremeWireless External Antenna Site Preparation and Installation Guide*](#)
- [*ExtremeWireless External Antenna with Wave 2 Site Preparation and Installation Guide*](#)
- [*ExtremeWireless Getting Started Guide*](#)
- [*ExtremeWireless Integration Guide*](#)
- [*ExtremeWireless Maintenance Guide*](#)
- [*ExtremeWireless Open Source Declaration*](#)
- [*ExtremeWireless User Guide*](#)
- [*IdentiFi Wireless WS-AP3865e Installation Guide*](#)
- [*IdentiFi Wireless WS-AP3825i & WS-AP3825e Installation Guide*](#)
- [*IdentiFi Wireless WS-AP3805i & WS-AP3805e Installation Guide*](#)



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 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.

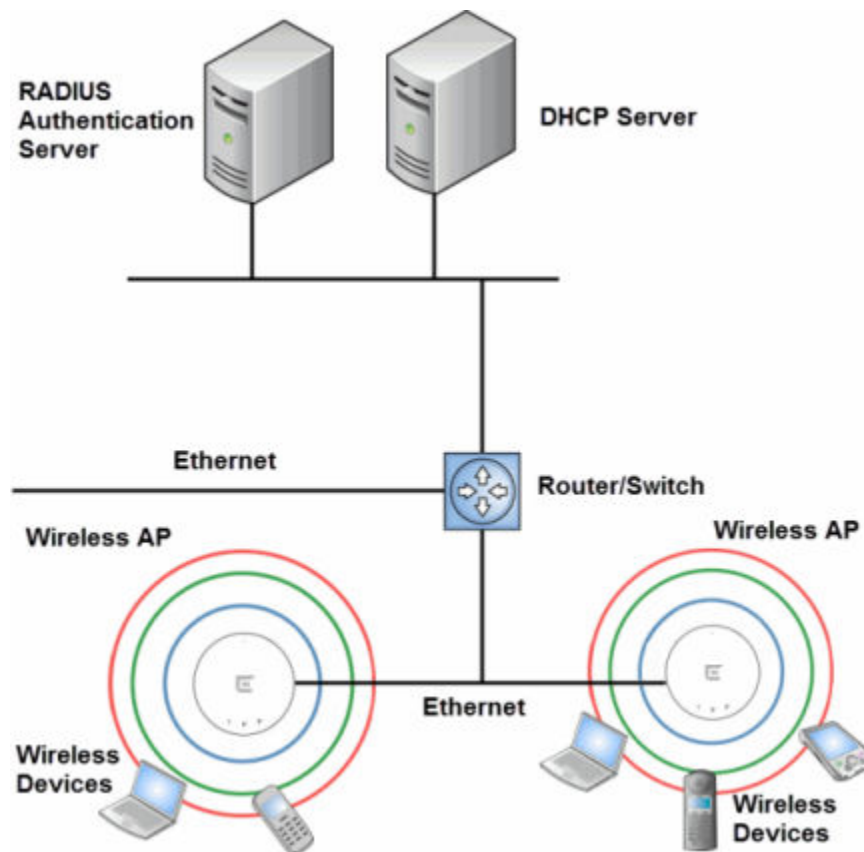


Figure 1: Standard Wireless Network Solution Example

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
- 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 52.
- SLP (Service Location Protocol)

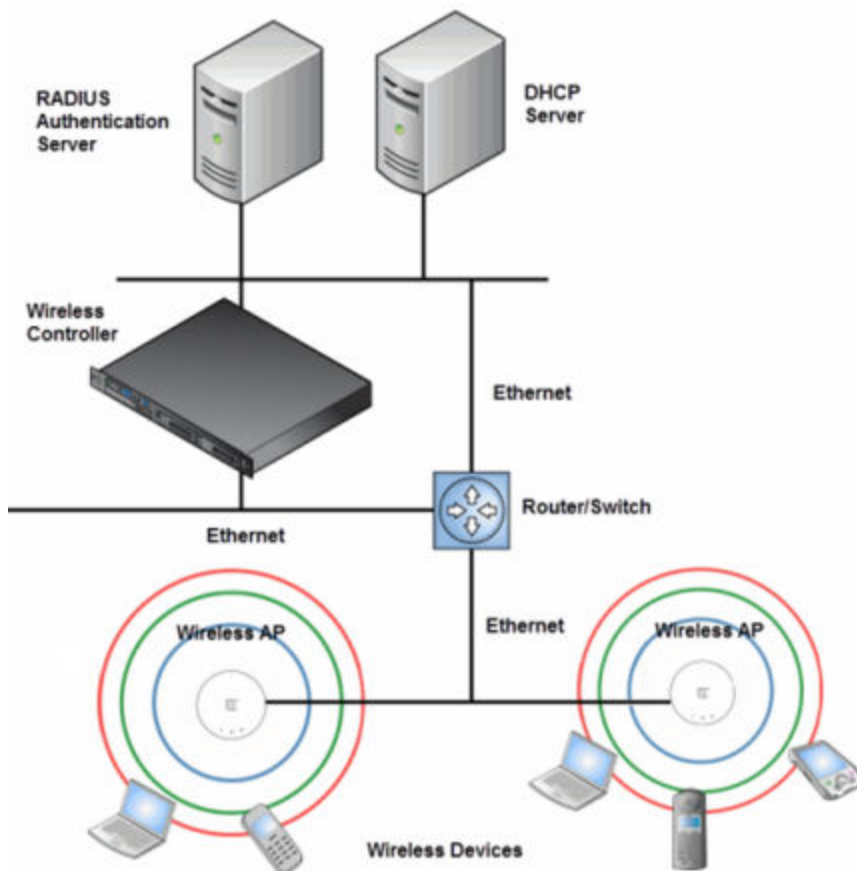


Figure 2: ExtremeWireless Appliance Solution

As illustrated in the above figure, 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:
 - 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, VLANs).
- Integrates with the Extreme Networks Extreme Management Center Suite of products. For more information, see [Extreme Networks Extreme Management Center Integration](#) on page 20.

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 [ExtremeWireless 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 [ExtremeWireless 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 26.
- 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.
- 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.
- Simple Network Management Protocol (SNMP) — 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 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.

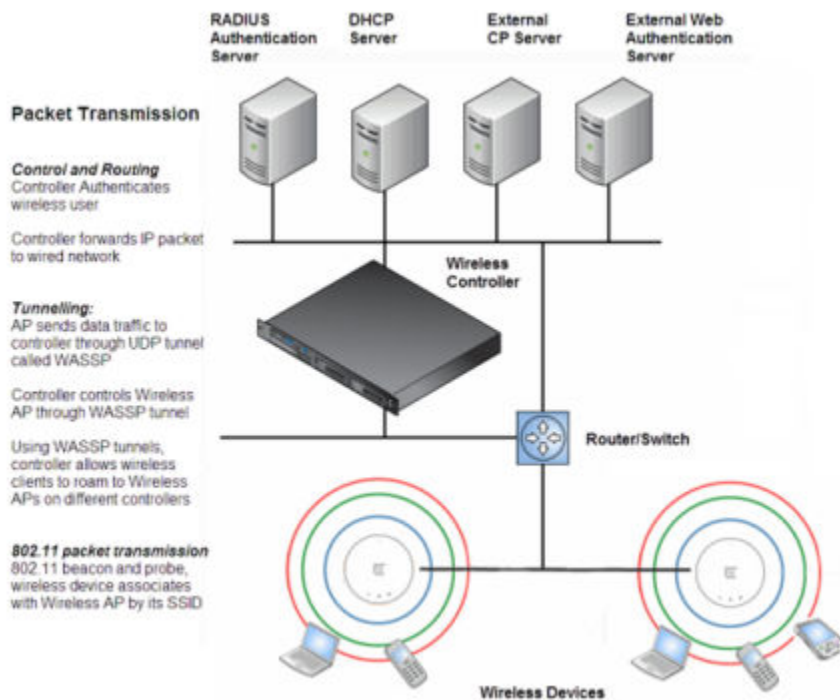


Figure 3: Traffic Flow Diagram

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.

The following figure illustrates the transition of the concept of a VNS to a binding of reusable components.

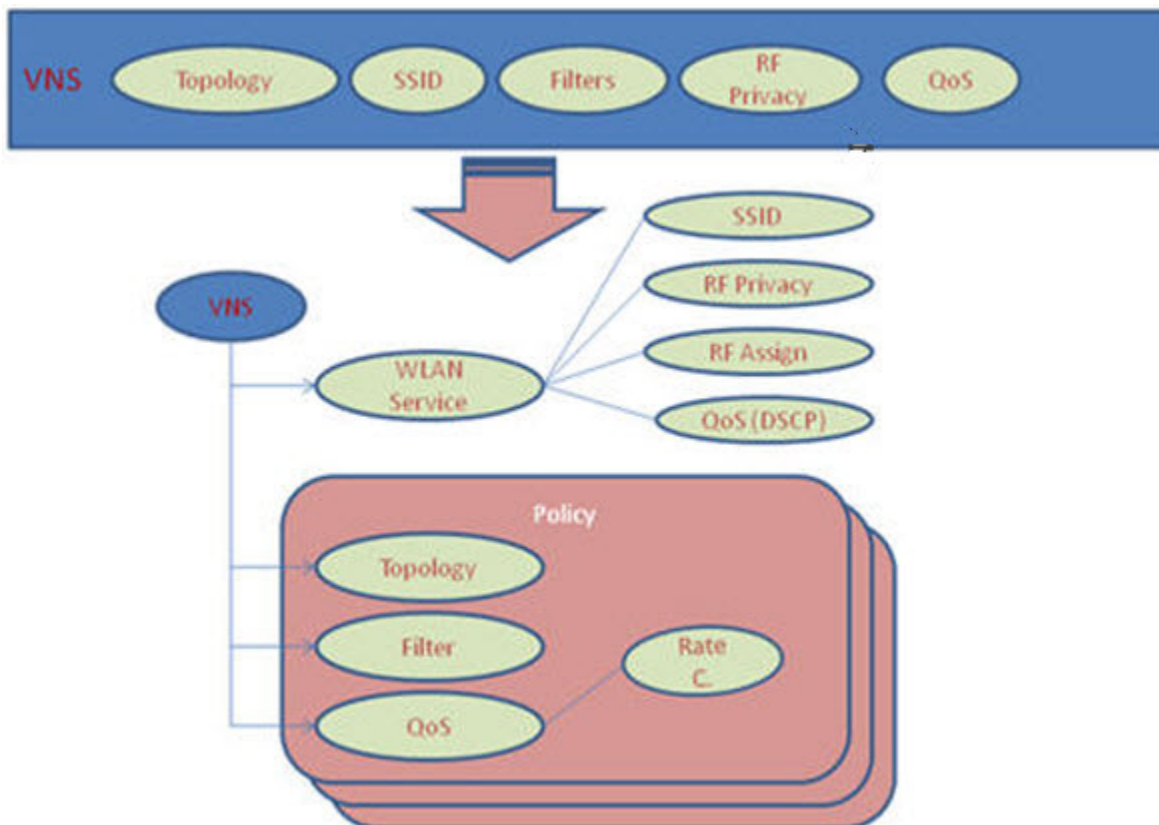


Figure 4: VNS as a Binding of Reusable Components

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 server to assign to wireless devices.

If the OSPF 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 WLANS 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
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.

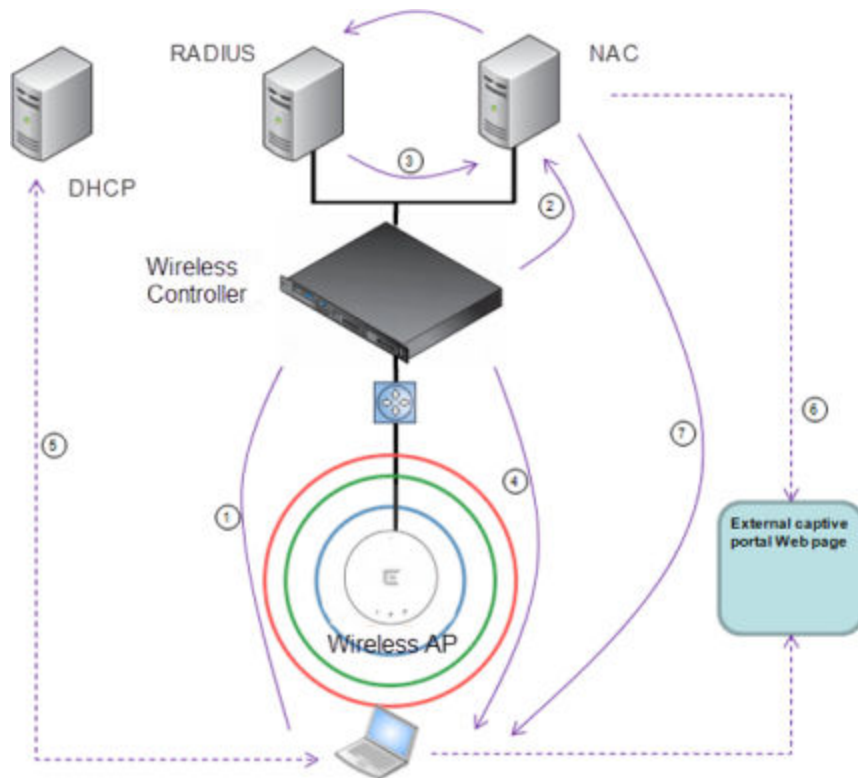
The AP3912 has three additional client ports that can be assigned to a single WLANS. For more information, see [Assigning WLAN Services to AP3912 Ports](#) on page 159.

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 376.



- 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 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.

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

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 226.

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, 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.
- Open Shortest Path First (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 checkbox.
- 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 Appliance 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	<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 deployment that is required. For example, topology and VLAN IDs, SSIDs, security requirements, and filter roles.
- 2 Prepare the network servers. Ensure that the external servers, such as 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 checkbox 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 88.

- 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 parameters, if appropriate to the network.

For more information, see [Configuring the ExtremeWireless Appliance for the First Time](#) on page 47.

- 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 223.
- 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)
 - Policies reference user's rate control profile.

For more information, see [Configuring Roles](#) on page 240.

- 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 273.

- 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 200.
- 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 98.
- 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.

- 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.



- 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.

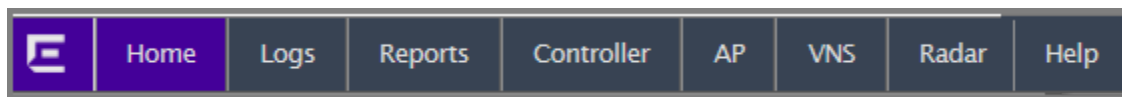


Figure 6: Wireless Assistant Top Menu Bar

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 74.</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 572.</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 572.</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 572.</p>

Table 5: Wireless Assistant Home Screen (continued)

Home Screen Heading	Description
Applications by WLAN	<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. <p>For more information, see Enabling Application Visibility with Device Identification on page 571 and Device Identification on page 570.</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 48). 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 519). 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 50.</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 572.</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 121, and Working with Radar Reports on page 542.</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 566.</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 35.
- 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:

- 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, 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** checkbox 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** checkbox 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** box, 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

- 1 In the **RADIUS** section, select the **Enable** checkbox 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** checkbox 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 509.
 - **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** checkbox to enable a default VNS for the controller.

**Note**

Refer to [Virtual Network Services](#) on page 24 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.

- 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 47
- [Applying Product License Keys](#) on page 48
- [Setting Up the Data Ports](#) on page 52
- [Setting Up Internal VLAN ID and Multicast Support](#) on page 59
- [Setting Up Static Routes](#) on page 60
- [Setting Up OSPF Routing](#) on page 62
- [Configuring Filtering at the Interface Level](#) on page 65
- [Protecting the Controller's Interfaces and Internal Captive Portal Page](#) on page 68
- [Configuring the Login Authentication Mode](#) on page 74
- [Configuring SNMP](#) on page 84
- [Configuring Network Time](#) on page 88
- [Configuring DNS Servers for Resolving Host Names of NTP and RADIUS Servers](#) on page 92

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** box, type the new administrator password.
- 5 In the **Confirm Password** box, 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 74.

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 two 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.



Note

You must obtain a specific permanent 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
- 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 519). 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

RADCAP025 — 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.

- **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 [following table](#) 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)
C4110	50	250	8

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
C5110	150	525	15
C5210	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 will start from the moment the first violation occurred. The controller will generate event logs for every violation. The only way to leave the grace period is to 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 will generate 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 490).

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.

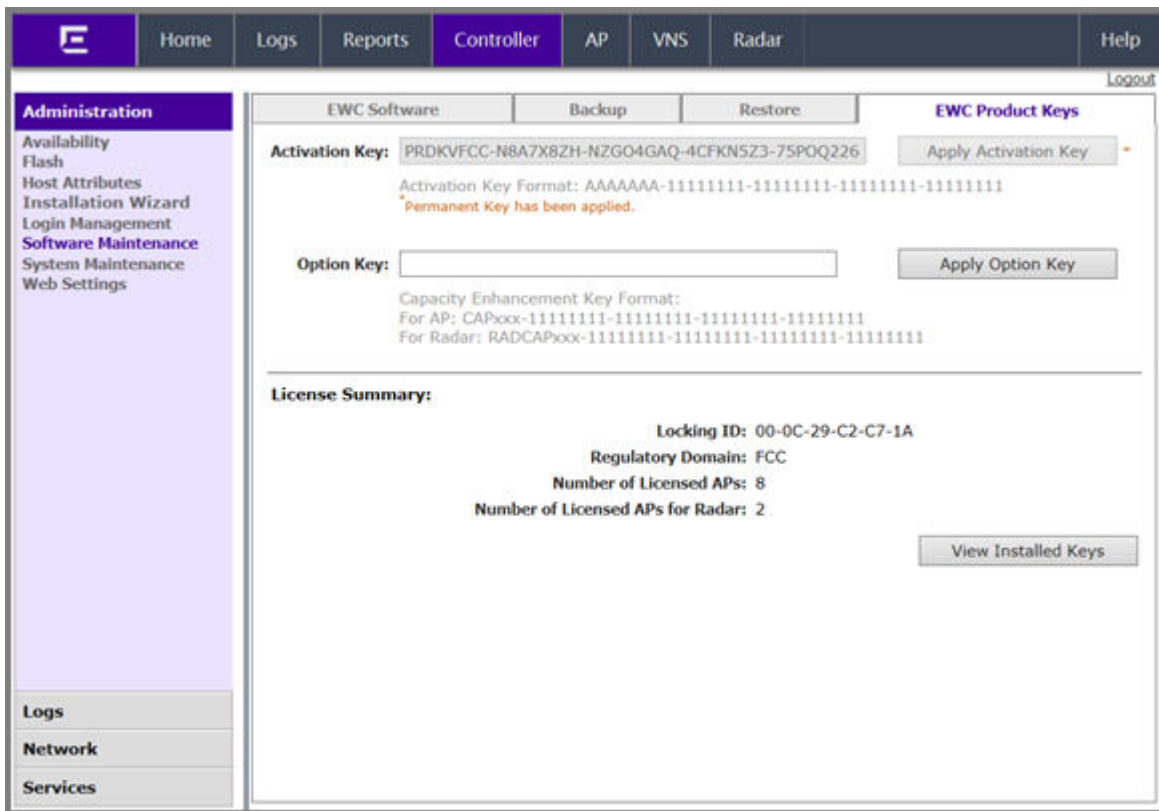


Figure 8: Product Keys Tab

- 4 If you are installing a temporary or permanent activation license key, type the key in the **Activation Key** box, and then click the **Apply Activation Key** button.
- 5 If you are installing a capacity enhancement, type the key in the **Option Key** box, 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 53.

Link Aggregation ports are represented by the L2 (peer-to-peer) 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 53.



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.

The screenshot shows the 'L2 Ports' configuration page. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. The left sidebar shows Administration, Logs, Network (selected), L2 Ports, Network Time, Routing Protocols, Secure Connections, SNMP, Topologies, and Utilities. The main content area is titled 'L2 Ports' and contains two tables.

Physical L2 Ports

Enable	Port	MAC	Untagged Vlan	Tagged Vlan
<input checked="" type="checkbox"/>	Port1	00:1B:21:8E:C6:10	4094	
<input checked="" type="checkbox"/>	Port2	00:1B:21:8E:C6:11		41, 42, 43
<input checked="" type="checkbox"/>	Port3	00:1B:21:8E:C6:14	4092	
<input checked="" type="checkbox"/>	Port4	00:1B:21:8E:C6:15	4091	
<input checked="" type="checkbox"/>	Admin	84:2B:2B:70:B9:4D	U	

Link Aggregation L2 Ports

Enable	Port	MAC	Untagged Vlan	Tagged Vlan	Attached Physical L2 Ports
<input checked="" type="checkbox"/>	lag1	00:1B:21:8E:C6:11			<input type="checkbox"/> Port1 <input type="checkbox"/> Port2 <input type="checkbox"/> Port3 <input type="checkbox"/> Port4
<input checked="" type="checkbox"/>	lag2	00:1B:21:8E:C6:11			<input type="checkbox"/> Port1 <input type="checkbox"/> Port2 <input type="checkbox"/> Port3 <input type="checkbox"/> Port4

Enable Jumbo Frames support ⓘ

*(U) is untagged vlan

Save

- 3 The **L2 Ports** tab presents the Physical (that is, Ethernet) and (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.
- 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.
 - 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 220.

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 checkbox.
- 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**. The **Topologies** tab is displayed.

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

The screenshot shows the 'Topologies' configuration page. The left sidebar contains 'Administration', 'Logs', 'Network', 'L2 Ports', 'Network Time', 'Routing Protocols', 'Secure Connections', 'SNMP', 'Topologies', and 'Utilities'. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The main content area is titled 'Topologies' and contains a table with the following data:

Topology Name	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	-	×	Admin	Static: 192.168.14.11 Dynamic IP Address	Admin
<input type="checkbox"/> Bridged at AP untagged	4093	×	-	-	B@AP
<input type="checkbox"/> CNL-422-0-0	4090	×	-	10.219.44.1	Routed
<input type="checkbox"/> CNL-422-0-1	4089	×	-	10.219.44.9	Routed
<input type="checkbox"/> CNL-422-0-2	42	✓	Port2	10.219.42.1	B@EWC
<input type="checkbox"/> CNL-422-0-3	4088	×	-	10.219.44.25	Routed
<input type="checkbox"/> CNL-422-1-2-wds	4087	×	-	-	B@AP
<input type="checkbox"/> CNL-422-1-4-wds	4086	×	-	-	B@AP

Below the table are buttons for 'New' and 'Delete Selected'. There are also input fields for 'Internal VLAN ID: 1' and 'Multicast Support: Port1'. A 'Save' button is located at the bottom right of the configuration area.

- To change any of the associated parameters, click on the topology entry to be modified. 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** checkbox.

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** box.
- 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** checkbox. 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** checkbox. 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 Server on the controller, in the **DHCP** box, 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.

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

- d In the **DNS Servers** box, type the DNS Server's IP address if you have a DNS Server.
- e In the **WINS** box, 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** boxes. Each entry must be separate by a comma. These two fields are not mandatory to enable the local DHCP feature.

- f In the **Gateway** box, 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** box, type the starting IP address of the IP address range.
 - In the **Address Range: to** box, 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.

- Select **Range**. In the **From** box, type the starting IP address of the IP address range that you want to exclude from the DHCP allocation.
- In the **To** box, 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 box.

- In the **Comment** box, 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** box.
 - To delete a IP Address from the exclusion list, select it in the **IP Address(es) to exclude from DHCP Range** box, and then click Delete.
 - To save your changes, click **OK**.
- a Click **Close** to close the **DHCP configuration** window.



Note

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

12 You are returned to the L2 port topology edit window.

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. The table below represents the data shown in the interface:

Topology Name	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	-	×	Admin	Static: 192.168.14.11 Dynamic IP Address	Admin
<input type="checkbox"/> Bridged at AP untagged	4093	×	-	-	B@AP
<input type="checkbox"/> CNL-422-0-0	4090	×	-	10.219.44.1	Routed
<input type="checkbox"/> CNL-422-0-1	4089	×	-	10.219.44.9	Routed
<input type="checkbox"/> CNL-422-0-2	42	✓	Port2	10.219.42.1	B@EWC
<input type="checkbox"/> CNL-422-0-3	4088	×	-	10.219.44.25	Routed
<input type="checkbox"/> CNL-422-1-2-wds	4087	×	-	-	B@AP
<input type="checkbox"/> CNL-422-1-4-wds	4086	×	-	-	B@AP

Below the table, there are buttons for 'New' and 'Delete Selected'. At the bottom, there are configuration fields: 'Internal VLAN ID: 1' and 'Multicast Support: Port1'. A 'Save' button is located at the bottom right of the configuration area.

- 3 In the **Internal VLAN ID** box, 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.

The screenshot shows the configuration interface for the ExtremeWireless Appliance. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. A Logout link is visible in the top right corner. The left sidebar contains a menu with categories: Administration, Logs, Network (selected), L2 Ports, Network Time, Routing Protocols (selected), Secure Connections, SNMP, Topologies, and Utilities. The main content area is titled 'Static Routes' and includes a 'View Forwarding Table' link and an 'OSPF' tab. Below this is a 'Route Settings' section containing a table with the following data:

R#	Dest.Addr	Subnet Mask	Gateway	Interface	O/D
<input type="checkbox"/>	0.0.0.0	0.0.0.0	10.219.40.2	Port1	off

Below the table are two buttons: 'New' and 'Delete Selected'.

- 3 To add a new route, click **New**, and in the **Edit route** dialog, enter the following information:
 - In the **Destination Address** box, 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** box, 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** box, 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** checkbox 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** checkbox.



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.

- 4 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:

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

- 3 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 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.

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

Setting Up OSPF Routing

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

- 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.
- Enable OSPF globally on the controller.
- Define the global OSPF parameters.

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 52).

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.

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.

The screenshot shows the OSPF configuration interface. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. The left sidebar shows Administration, Logs, Network (selected), L2 Ports, Network Time, Routing Protocols (selected), Secure Connections, SNMP, Topologies, and Utilities. The main content area is titled 'View Forwarding Table' and contains the following settings:

Global Settings

OSPF Status: On (dropdown) Area id: 0.0.0.2 (text box)
 Router id: (text box) Area Type: Default (dropdown) Save (button)

Interface Settings

Topology	Enabled	Authentication	Password	Cost	H / I	D / I	RT / I	Delay
<input type="checkbox"/> Port1	Enabled	None		10	10	40	5	1
<input type="checkbox"/> Port2	Disabled	None		10	10	40	5	1
<input type="checkbox"/> Port3	Disabled	None		10	10	40	5	1
<input type="checkbox"/> Port4	Disabled	None		10	10	40	5	1

New (button) Delete Selected (button)

- 4 From the **OSPF Status** drop-down list, click **On** to enable OSPF.
 In the **Router ID** box, 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** box, 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**.
 To Set OSPF Routing Port Settings on the Controller:
- 8 In the left pane, click **Network** > **Routing Protocols**.
- 9 Click the **OSPF** tab.

- 10 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.

Edit Port [?] [X]

Topology: phy2

Link Cost: 50001

Authentication: None ▼

Password: []

Port Status:

Hello Interval: 10 (s)

Dead Interval: 40 (s)

Retransmit Interval: 5 (s)

Transmit Delay: 1 (s)

[Save] [Cancel]

- 11 In the **Link Cost** box, 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 243.

- 12 In the **Authentication** drop-down list, click the authentication type for OSPF on your network: **None** or **Password**. The default setting is **None**.
- 13 If **Password** is selected as the authentication type, in the **Password** box, type the password. If **None** is selected as the Authentication type, leave this box empty. This password must match on either end of the OSPF connection.
- 14 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.
- 15 To save your changes, click **Save**.
- To Confirm That Ports Are Set for OSPF:

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

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

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	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	-	×	Admin	Static: 192.168.14.11 Dynamic IP Address	Admin
<input type="checkbox"/> Bridged at AP untagged	4093	×	-	-	B@AP
<input type="checkbox"/> CNL-422-0-0	4090	×	-	10.219.44.1	Routed
<input type="checkbox"/> CNL-422-0-1	4089	×	-	10.219.44.9	Routed
<input type="checkbox"/> CNL-422-0-2	42	✓	Port2	10.219.42.1	B@EWC
<input type="checkbox"/> CNL-422-0-3	4088	×	-	10.219.44.25	Routed
<input type="checkbox"/> CNL-422-1-2-wds	4087	×	-	-	B@AP
<input type="checkbox"/> CNL-422-1-4-wds	4086	×	-	-	B@AP

- 3 On the **Topologies** tab, click the appropriate data port topology. The **Edit Topology** window displays.
- 4 Select the **Management Traffic** checkbox 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 243.

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

Edit Topology [?] [X]

Topology: CNL-422-0-1

General | Multicast Filters | **Exception Filters**

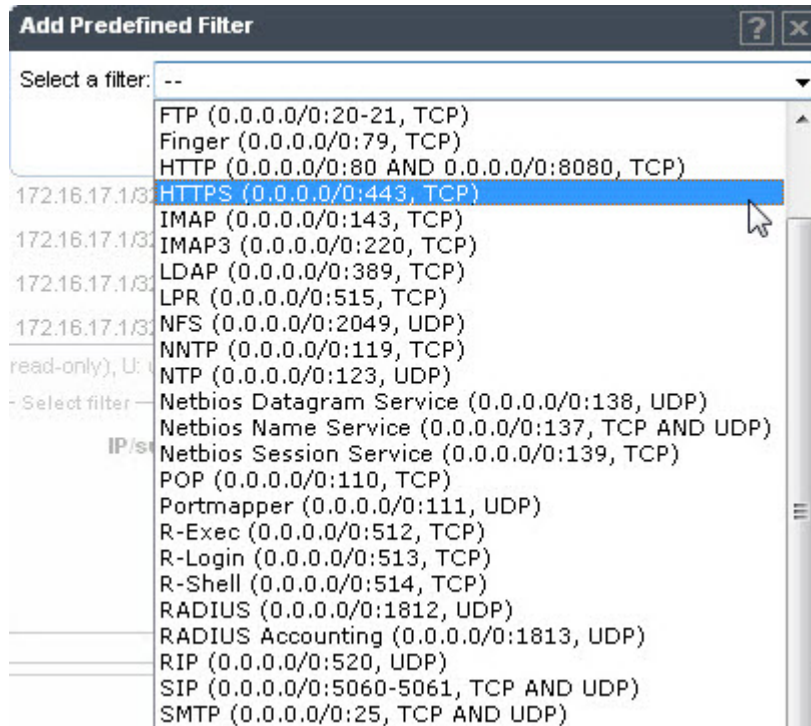
Rule	In	Allow	IP : Port	Protocol
I	dest	<input type="checkbox"/>	10.219.44.9/32:60606	TCP
I	dest	<input type="checkbox"/>	0.0.0.0/32:50200	TCP
I	dest	<input checked="" type="checkbox"/>	10.219.44.9/32:32768-65535	TCP
I	dest	<input checked="" type="checkbox"/>	10.219.44.9/32:32768-65535	UDP
I	dest	<input checked="" type="checkbox"/>	10.219.44.9/32:67 (DHCP Server)	UDP
I	dest	<input checked="" type="checkbox"/>	255.255.255.255/32:67 (DHCP Server)	UDP
I	dest	<input checked="" type="checkbox"/>	10.219.44.9/32	ICMP
I	dest	<input type="checkbox"/>	0.0.0.0/0	N/A

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

Select filter

IP/subnet:port: 0.0.0.0/0
 Protocol: N/A
 In Filter: Destination(dest)

- 5 Add rules by either:
 - Clicking the **Add Predefined** button, selecting a filter from the drop down list, and clicking **Add**.



- Clicking the Add button, filling in the following fields, then clicking **OK**:

In the **IP / subnet:port** box, 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, . 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** checkbox.
- 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 the Controller's Interfaces and 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.



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).

The **Configuration for Topologies** section displays.

Table 8: Topologies Page: Certificates Tab Fields and Buttons

Field/Button	Description
Interface Certificates	
Topology	Topology name
Expiry Date	Date when the certificate expires
CA Cert.	Identifies whether or not a CA certificate has been installed on the topology.

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

Field/Button	Description
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	To replace/install the existing port's certificate and key using this option, do the following: <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 box. 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 box. 9 (Optional) Click Browse next to the Optional:Enter PEM-encoded CA public certificates file box. 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 box. <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 box. 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 box. 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 box. 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 box. <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 box. 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 box. 3 Click Browse next to the Private key file to install box. 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 box. 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 box. 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 box. <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 74.
- RADIUS authentication — The controller uses login credentials and passwords configured on a RADIUS server. See [Configuring the RADIUS Login Authentication Mode](#) on page 76.
- 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 80.
- 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 82.



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 618.

To configure the 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' configuration page. The left sidebar contains 'Administration' > 'Login Management'. The main content area is divided into 'Local Authentication' and 'RADIUS Authentication' tabs. Under 'Local Authentication', there are three user groups: 'Full Administrator', 'Read-only Administrator', and 'GuestPortal Manager'. The 'admin' user is listed under 'Full Administrator'. The 'Add User' section has a 'Group' dropdown set to 'Full Administrator', and fields for 'User ID', 'Password', and 'Confirm Password'. The 'Modify User' section has a 'User ID' field set to 'admin', and fields for 'Password' and 'Confirm Password'. The 'Authentication mode' is set to 'RADIUS, Local'. Buttons for 'Add User', 'Change Password', 'Remove user', 'Reset', 'Configure', and 'Save' are visible.

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

The 'Login Authentication Mode Configuration' dialog box is shown. It contains a table with two columns: 'Enable' and 'Authentication'. The 'Local' row has a checked checkbox, and the 'RADIUS' row has an unchecked checkbox. There are 'Move Up' and 'Move Down' buttons to the right of the table, and 'OK' and 'Cancel' buttons at the bottom.

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

- 4 Select the **Local** checkbox.
If the RADIUS checkbox is selected, deselect it.
- 5 **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 345.

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.

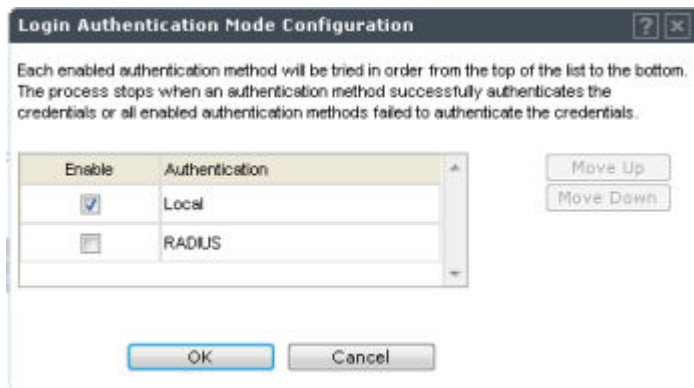
To configure the RADIUS login authentication mode:

- 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 shows the web interface for configuring RADIUS Authentication. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. The left sidebar shows the Administration menu with Login Management selected. The main content area has two tabs: Local Authentication and RADIUS Authentication (selected). Under RADIUS Authentication, there is a 'Use' button, a 'Configured Servers' list with one entry 'Smoke Test Radius Ser' and 'Up/Down' buttons, and a 'Test' button. A 'View Summary' button is also present. A 'Auth +' section contains a checked box for 'Use server for Authentication', with fields for 'NAS IP Address: 10.219.40.1', 'NAS identifier: lab-422-g', and 'Auth. type: CHAP'. A 'Reset' button is at the bottom right of this section. At the bottom of the page, the 'Authentication mode' is set to 'RADIUS, Local', with 'Configure' and 'Save' buttons.

- 4 In the **Authentication mode** section, click **Configure**.

The **Login Authentication Mode Configuration** window is displayed.



- 5 Select the **RADIUS** checkbox.
If the **Local** checkbox is selected, deselect it.
- 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 345.

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.

- 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".

- In the **User ID** and the **Password** boxes, 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.

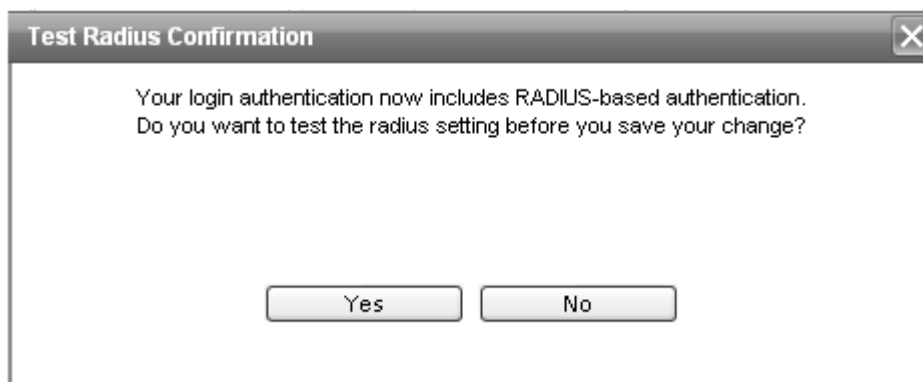
The screenshot shows the same "Test RADIUS Servers" dialog box, but now it displays the results. The text "RADIUS Test Results:" is followed by "Successful". A "Close" button is centered at the bottom of the dialog.

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**.

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

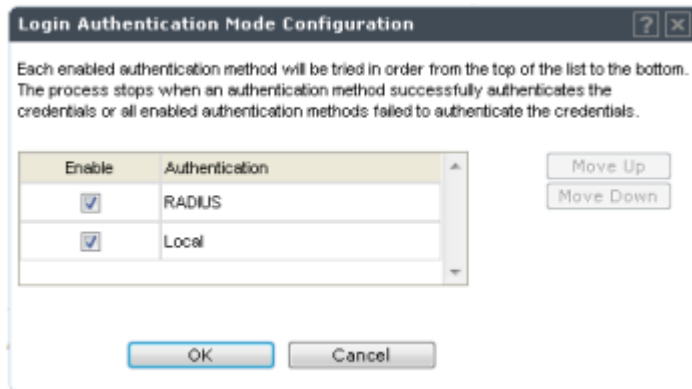
The screenshot shows the web interface for configuring login management. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. A left sidebar contains the Administration menu with options like Availability, Flash, Host Attributes, Installation Wizard, Login Management (selected), Software Maintenance, System Maintenance, and Web Settings. The main content area is titled 'Local Authentication' and 'RADIUS Authentication'. It features a table of user roles: Full Administrator (with an 'admin' user listed), Read-only Administrator, and GuestPortal Manager. To the right, there are sections for 'Add User' and 'Modify User', each with input fields for Group, User ID, Password, and Confirm Password, and buttons for 'Add User', 'Change Password', 'Remove user', and 'Reset'. At the bottom, the 'Authentication mode' is set to 'RADIUS, Local', with 'Configure' and 'Save' buttons.

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

The screenshot shows the 'Login Authentication Mode Configuration' dialog box. It contains a list of authentication methods with checkboxes for enabling them. The 'RADIUS' method is checked, and 'Local' is unchecked. There are 'Move Up' and 'Move Down' buttons to the right of the list. At the bottom, there are 'OK' and 'Cancel' buttons. The dialog also includes a help icon and a close button in the title bar.

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

- 4 Select the **Local** and **RADIUS** checkbox.



- 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 74.

For information on setting RADIUS login authentication settings, see [Configuring the RADIUS Login Authentication Mode](#) on page 76.

Configuring the RADIUS, Local Login Authentication Mode

To configure the RADIUS, Local login authentication mode:

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

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

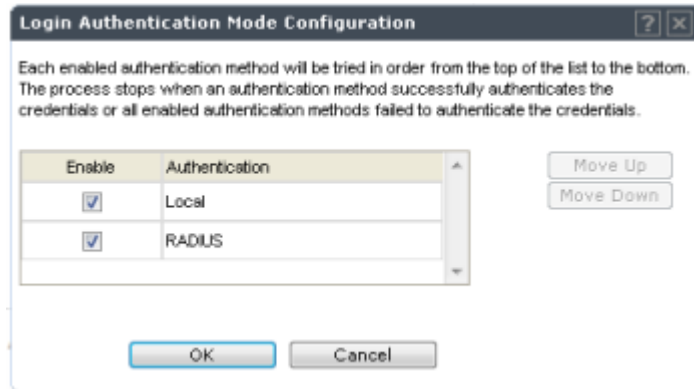
The screenshot shows the web interface for configuring login management. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. A left sidebar contains Administration (selected), Availability, Flash, Host Attributes, Installation Wizard, Login Management (selected), Software Maintenance, System Maintenance, and Web Settings. Below the sidebar are sections for Logs, Network, and Services. The main content area is titled 'Local Authentication' and 'RADIUS Authentication'. It features a list of user roles: Full Administrator (with an 'admin' user listed), Read-only Administrator, and GuestPortal Manager. To the right, there are sections for 'Add User' and 'Modify User'. The 'Add User' section includes a dropdown for 'Group' (set to 'Full Administrator'), and input fields for 'User ID', 'Password', and 'Confirm Password', followed by an 'Add User' button. The 'Modify User' section includes an input field for 'User ID' (set to 'admin'), and input fields for 'Password' and 'Confirm Password', followed by 'Change Password', 'Remove user', and 'Reset' buttons. At the bottom, the 'Authentication mode' is set to 'RADIUS, Local', with 'Configure' and 'Save' buttons.

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

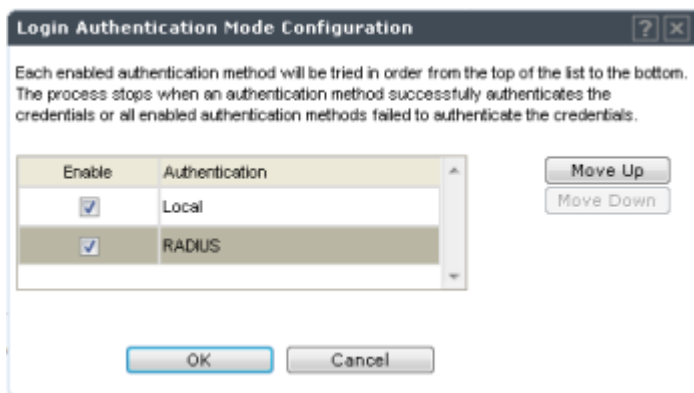
The screenshot shows the 'Login Authentication Mode Configuration' dialog box. It contains a text box explaining that each enabled authentication method will be tried in order from top to bottom, and the process stops when successful or all methods fail. Below this is a table with two columns: 'Enable' and 'Authentication'. The 'Local' method is checked, and the 'RADIUS' method is unchecked. To the right of the table are 'Move Up' and 'Move Down' buttons. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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

- 4 Select the **Local** and **RADIUS** checkbox.



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



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

For information on setting RADIUS login authentication settings, see [Configuring the RADIUS Login Authentication Mode](#) on page 76.

For information on setting local login authentication settings, see [Configuring the Local Login Authentication Mode and Adding New Users](#) on page 74.

Configuring SNMP

The controller supports the Simple Network Management Protocol (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:

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

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

The screenshot displays the 'SNMP Common Settings' configuration page. The left navigation pane shows 'Network' > 'SNMP' selected. The main content area is titled 'SNMP Common Settings' and includes the following fields:

- Mode:** Radio buttons for No SNMP, SNMPv1/v2c, and SNMPv3.
- Contact Name:** Text input field containing 'Lucy Kestekian'.
- Location:** Text input field containing 'lab-422'.
- SNMP Port:** Text input field containing '162'.
- Forward Traps:** Dropdown menu set to 'Informational'.
- Publish AP as interface of controller:** Dropdown menu set to 'Enabled'.

Below these settings are two tabs: 'SNMPv1/v2c' (selected) and 'SNMPv3'. The 'SNMPv1/v2c' tab contains the following fields:

- Read Community Name:** Text input field containing 'public'.
- Read/Write Community Name:** Text input field containing 'private'.
- Manager A:** Text input field containing '136.157.233.176'.
- Manager B:** Text input field containing '192.168.3.100'.

A 'Save' button is located at the bottom right of the configuration area.

- 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 86
 - [Configuring SNMPv3-specific Parameters](#) on page 86

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 SnmpEngineID 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: , 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 566.

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

To configure 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.

The screenshot shows the 'Network Time' configuration page. The left navigation pane is expanded to 'Network Time'. The main content area is titled 'Network Time' and contains the following sections:

- Time Zone Settings***:
 - Continent or Ocean: America (dropdown)
 - Time Zone Region: Montreal (dropdown)
 - Apply Time Zone button
 - *Time Zone changes may take up to 60 seconds to take effect
- System Time**:
 - 01-20-2017 11:06 (mm-dd-yyyy hh:mm)
 - Set Clock button
- NTP** (checked):
 - Time Server 1: [input field]
 - Time Server 2: [input field]
 - Time Server 3: [input field]
 - Run local NTP Server (checked)
 - Apply button

- 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** box, 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

To configure 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.

The screenshot shows the 'Network Time' configuration page. The left sidebar has 'Network' selected, with 'Network Time' highlighted. The main content area is titled 'Network Time' and contains the following sections:

- Time Zone Settings***:
 - Continent or Ocean: America (dropdown)
 - Time Zone Region: Montreal (dropdown)
 - Apply Time Zone button
 - *Time Zone changes may take up to 60 seconds to take effect
- System Time**: 01-20-2017 11:06 (mm-dd-yyyy hh:mm) with a Set Clock button.
- NTP**:
 - Checked checkbox
 - Time Server 1: [text box]
 - Time Server 2: [text box]
 - Time Server 3: [text box]
 - Run local NTP Server: checked checkbox
 - Apply button

- 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** checkbox.



Note

If you want to use the controller as the NTP Server, select the **Run local NTP Server** checkbox, 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**.
- 2 In the left pane, click **Network > Secure Connections**. The **Secure Connections** screen displays.

The screenshot shows the configuration interface for the Controller. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. A Logout link is visible in the top right. The left sidebar shows a tree view with Administration, Logs, Network (selected), L2 Ports, Network Time, Routing Protocols, Secure Connections (highlighted), SNMP, Topologies, and Utilities. The main content area is titled 'Shared Secret for Remote Connections' and features a checkbox for 'Enable Weak Ciphers' which is checked. Below this is a table with two columns: 'Peer IP Address' and 'Shared Secret'. At the bottom of the table, there are two input fields and an 'Add / Update' button. Below the input fields are three buttons: 'Show Shared Secrets', 'Remove Selected Peer', and 'Save'.

- 3 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.
- 4 Enter the Server IP address of the other end of the secure protocol tunnel and the shared secret to use.
- 5 Click **Add/Update**.

- 6 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 346.

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**.

- 2 In the left pane, click **Administration** > **Host Attributes**. The **Host Attributes** screen displays.

The screenshot shows the 'Host Attributes' configuration page. The left sidebar has 'Administration' selected, with 'Host Attributes' highlighted. The main content area is divided into sections: 'Network Identification' with 'Host Name' (CS210) and 'Domain Name' (extremenetworks.com); 'DNS' with a list of servers (192.168.11.21), a 'Server Address' field (192.168.11.21), and buttons for 'Add Server', 'Remove selected server', and 'Move up'; and 'Default Gateway IP' (10.49.224.1). A 'Save' button is at the bottom right. The status bar at the bottom shows system information like 'CS210 | CS210 | 00 days, 04:07 | User: admin' and software version '10.01.01.0081'.

- 3 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.

- 4 In the **Default Gateway IP** box, enter the IP address of the Default Gateway.
5 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 604.

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 94

[AP Multi-Edit Properties](#) on page 110

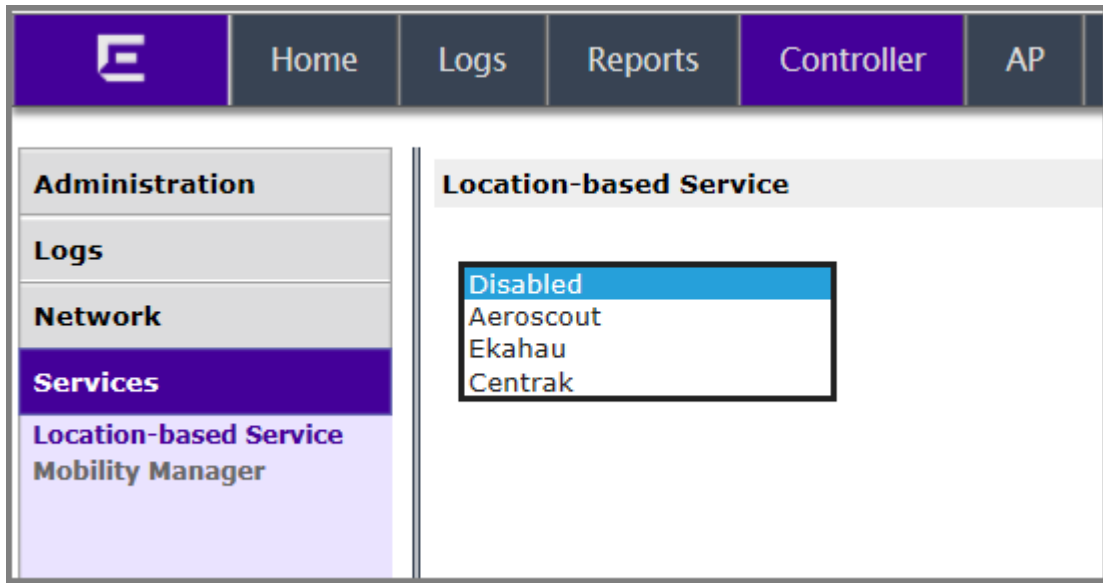
[AP Properties Tab - Advanced Settings](#) on page 154

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**.



- 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"/>	0000000C29AC00AB	AP3715i		/World/Thornhill	10.11.01.0183T	Local
<input type="checkbox"/>	13310618085D0000	AP3715e			10.11.01.0183T	Local
<input type="checkbox"/>	2935	AP3825i			10.11.01.0183T	Local
<input type="checkbox"/>	3705i	AP3705i			10.11.01.0183T	Local
<input type="checkbox"/>	3801i	AP3801i			10.11.01.0183T	Local
<input type="checkbox"/>	3805	AP3805i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3825i	AP3825i			10.11.01.0183T	Local
<input type="checkbox"/>	3865e-1	AP3865e			10.11.01.0183T	Local
<input type="checkbox"/>	39350000000000e1	AP3935e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	39350000000000i1	AP3935i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3935ssdfafafa111	AP3715e			10.11.01.0183T	Local
<input type="checkbox"/>	39650000000000e1	AP3965e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	39650000000000i1	AP3965i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3965e	AP3965e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	ap3805 fcc	AP3805i-FCC			10.11.01.0183T	Local

Showing: 17 rows, Local: 17

- 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 93
- [AP Multi-Edit Properties](#) on page 110
- [AP Properties Tab - Advanced Settings](#) on page 154

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 615 or the Extreme Networks *ExtremeWireless Maintenance Guide*.

4 Configuring the ExtremeWireless APs

Wireless AP Overview
Discovery and Registration
Wireless AP Default Configuration
Configuring Wireless AP Properties
Assigning Wireless AP Radios to a VNS
Configuring Wireless AP Radio Properties
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
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 AP. 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 Nomenclature

The following table lists ExtremeWireless APs supported. AP models are listed in the order of most current models (top) to the oldest models (bottom), with the next-generation 39xx APs being the most recent product series.

Table 10: ExtremeWireless APs

AP Series	Product Number	Product Description	Product Long Description	XCloud Support
AP3912 -Cloud-ready, Wall-plate, Dual band, Dual Radio 802.11ac/abgn, 2x2:2 MIMO Indoor Wave 2 access point that offers a range of connectivity options, including three policy controllable wired LAN ports (2.4/5G) and a wired pass-through port.	31025	WS-AP3912i-FCC	Includes a four internal antenna array. Restricted Regulatory Domain: FCC (Available in the U.S., Puerto Rico, and Colombia).	Yes
	31026	WS-AP3912i-ROW	Includes a four internal antenna array. Restricted Regulatory Domain: ROW (Available in regions other than U.S., Puerto Rico, and Colombia).	Yes
AP3935 -Dual band, Dual Radio 802.11ac/abgn, 4x4:4 MIMO Indoor Wave 2 access points.	31012	WS-AP3935i-FCC	Includes an eight internal antenna array and active/active E/N data ports. Restricted Regulatory Domain: FCC (Available in the U.S., Puerto Rico, and Colombia).	Yes
	31013	WS-AP3935i-ROW	Includes an eight internal antenna array and active/active E/N data ports. Restricted Regulatory Domain: ROW (Available in regions other than U.S., Puerto Rico, and Colombia).	Yes
	31014	WS-AP3935e-FCC	Includes eight, external, N-type jack connectors (4 connectors per band) for external antenna array and active/active E/N data ports. Regulatory Domain: FCC (Available in the U.S., Puerto Rico, and Colombia).	No

Table 10: ExtremeWireless APs (continued)

AP Series	Product Number	Product Description	Product Long Description	XCloud Support
	31015	WS-AP3935e-ROW	Includes eight, external, N-type jack connectors (4 connectors per band) for external antenna array and active/active E/N data ports. Regulatory Domain: ROW (Available in regions other than U.S., Puerto Rico, and Colombia).	No
	31020	WS-AP3935i-IL	Includes an eight internal antenna array and active/active E/N data ports. Restricted Regulatory Domain: IL (Available in Isreal).	Yes
AP3965 - Dual band, Dual Radio 802.11ac/abgn, 4x4:4 MIMO Outdoor Wave 2 access points.	31016	WS-AP3965i-FCC	Includes an eight internal antenna array and active/active E/N data ports. Restricted Regulatory Domain: FCC (Available in the U.S., Puerto Rico, and Colombia).	Yes
	31017	WS-AP3965i-ROW	Includes an eight internal antenna array and active/active E/N data ports. Regulatory Domain: ROW (Available in regions other than the U.S., Puerto Rico, and Colombia).	Yes

Table 10: ExtremeWireless APs (continued)

AP Series	Product Number	Product Description	Product Long Description	XCloud Support
	31018	WS-AP3965e-FCC	Includes eight, external, N-type jack connectors (4 connectors per band) for external antenna array and active/active E/N data ports. Regulatory Domain: FCC (Available in the U.S., Puerto Rico, and Colombia).	No
	31019	WS-AP3965e-ROW	Includes eight, external, N-type jack connectors (4 connectors per band) for external antenna array and active/active E/N data ports. Regulatory Domain: ROW (Available in regions other than the U.S., Puerto Rico, and Colombia).	No
AP3805 - Dual band, Dual Radio 802.11ac/abgn, 2x2:2 MIMO Indoor Wave 1 access points.	30912	WS-AP3805i-FCC	Includes four internal antenna array. Restricted Regulatory Domain: FCC (Available in the U.S., Puerto Rico, and Colombia).	Yes
	30913	WS-AP3805i-ROW	Includes four internal antenna array. Restricted Regulatory Domain: ROW (Available in regions other than U.S., Puerto Rico, and Colombia).	Yes
	WS-AP3805i	WS-AP3805i	Indoor AP with internal antenna assemblies. Supports the 802.11ac wireless standards.	No
	WS-AP3805e	WS-AP3805e	Indoor AP with external antenna connectors. Supports the 802.11ac wireless standards.	No

Table 10: ExtremeWireless APs (continued)

AP Series	Product Number	Product Description	Product Long Description	XCloud Support
	WS-AP3805i	WS-AP3805i	Indoor AP with internal antenna assemblies. Supports the 802.11ac wireless standards. Mfg rev 5K or greater.	No
	WS-AP3805e	WS-AP3805e	Indoor AP with external antenna connectors. Supports the 802.11ac wireless standards. Mfg rev 5K or greater.	No
AP3801	WS-AP3801i	WS-AP3801i	Indoor AP with internal antenna assemblies. Supports the 802.11ac wireless standards.	No
	WS-AP3801i	WS-AP3801i	Indoor AP with internal antenna assemblies. Supports the 802.11ac wireless standards. (Mfg rev 5F or greater).	No
AP3825	WS-AP3825i	WS-AP3825i	Indoor AP with internal antenna assemblies. Supports the 802.11ac and 802.11n wireless standards.	No
	WS-AP3825e	WS-AP3825e	Indoor AP with external antenna connectors. Supports the 802.11ac and 802.11n wireless standards.	No
	WS-AP3825i	WS-AP3825i-1	Indoor AP with internal antenna assemblies. Supports the 802.11ac and 802.11n wireless standards. App ID WS-3825i-1 (mfg rev 5L or greater). Units produced after May 2016.	No

Table 10: ExtremeWireless APs (continued)

AP Series	Product Number	Product Description	Product Long Description	XCloud Support
	WS-AP3825e	WS-AP3825e-1	Indoor AP with external antenna connectors. Supports the 802.11ac and 802.11n wireless standards. App ID WS-3825e-1 (mfg rev 5L or greater). Units produced after May 2016.	No
AP3865	WS-AP3865e	WS-AP3865e	Outdoor AP with external antenna assemblies. Supports the 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac protocols.	No
AP3705	WS-AP3705i	WS-AP3705i	Indoor AP with internal antennas, 2x2x2 802.11abgn	No
AP3710	WS-AP3710i	WS-AP3710i	Indoor AP with internal antennas, 3x3x3 802.11abgn	No
	WS-AP3710e	WS-AP3710e	Indoor AP with external antennas, 3x3x3 802.11abgn	No
AP3715	WS-AP3715i	WS-AP3715i	Indoor AP with internal antennas, 3x3x3 802.11abgn	No
	WS-AP3715e	WS-AP3715e	Indoor AP with external antennas, 3x3x3 802.11abgn	No
AP3765	WS-AP3765i	WS-AP3765i	Outdoor AP with internal antennas, 3x3x3 802.11ac, 802.11abgn	No
	WS-AP3765e	WS-AP3765e	Outdoor AP with external antennas, 3x3x3 802.11ac, 802.11abgn	No
AP3767	WS-AP3767e	WS-AP3767e	Outdoor AP with external antennas, 3x3x3, 802.11n, 802.11a/b/g	No

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.

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 172.

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. For a list of the external antennas that can be used with each AP model and how to install them, refer 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 147.

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.
- 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.

- **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 517.

Other differentiating features in an AP product series are the number of internal or external antennas (see [Antennas](#) on page 104), or the number of radios the AP has (see [Radios](#) on page 105).

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

The 39xx, 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 163.

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 172.

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 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 all the 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. The AP cannot scan or transmit on channels that are prohibited by the regulations of the countries in which it is deployed.

Radar feature configuration is described in [Working with ExtremeWireless Radar](#) on page 517.

802.11n- and 802.11ac-Compliant Access Point Features

All 802.11n-compatible APs have the following features. Pre-802.11n generation APs do not have these 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.

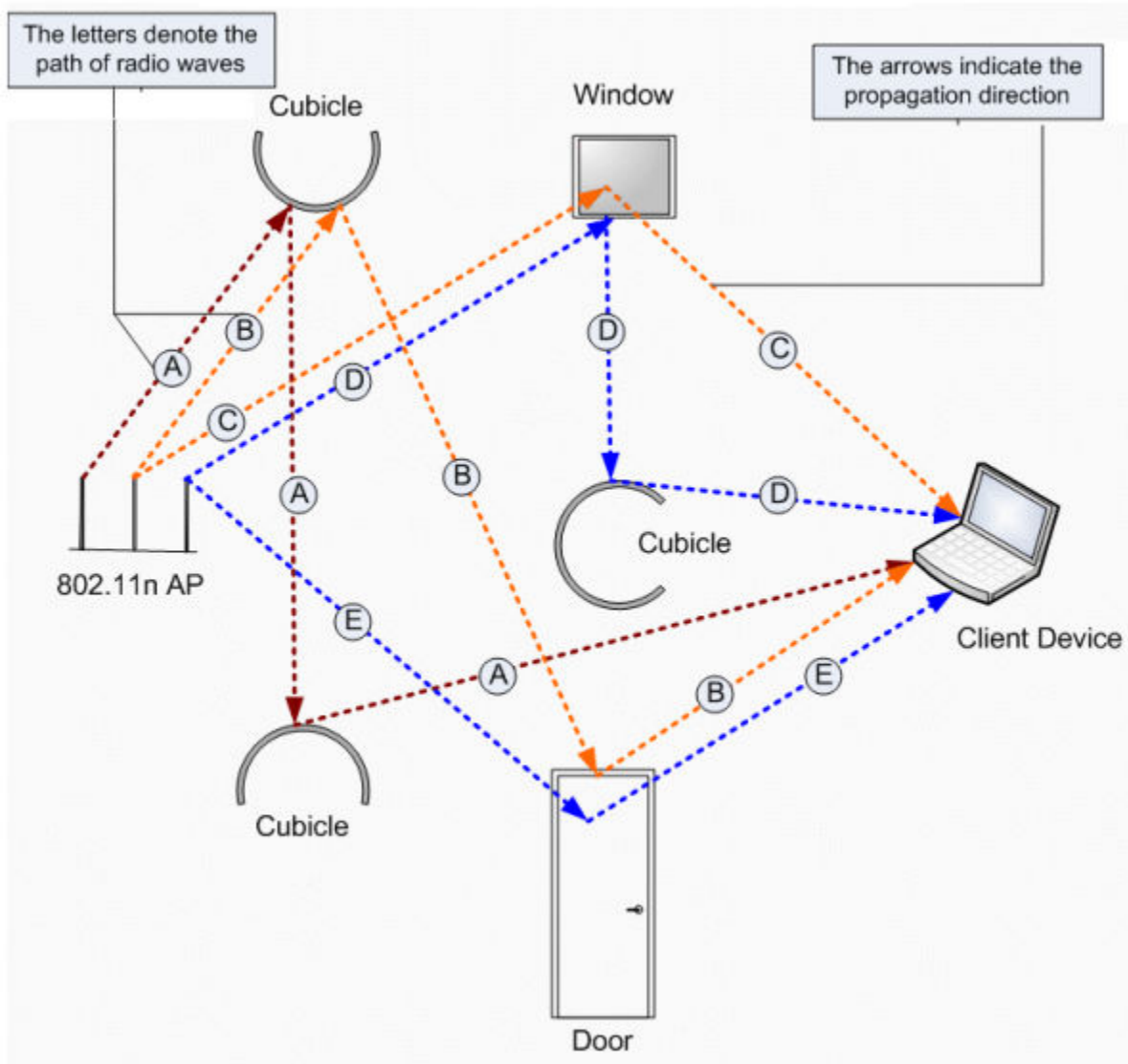
MIMO radios send out one, two or three radio signals through each antenna. Each signal is called a spatial stream. The antennas on the AP are deliberately spaced so that each spatial stream follows a slightly different path to the client device. Two spatial streams get multiplied into several streams 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 antennas 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 650.

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 147.

Licensing Considerations

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

- FCC
- ROW
- MNT

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

- A wireless controller with an FCC license can manage Access Points deployed in the United States, Puerto Rico, or Colombia.
- A wireless controller with a ROW license can manage Access Points deployed in any country *except* the United States, Puerto Rico, 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 *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 119.

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 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 119.

- **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 109.

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 173 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 33.

- The ExtremeWireless Appliance has been configured. For more information, see [Configuring the ExtremeWireless Appliance](#) on page 33.
- 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 121.
- 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 11: 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 557) 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 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.</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 498.</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 11: Multi-Edit AP Properties (continued)

Field	Description
Secure Tunnel Lifetime (hours)	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	Determines if the AP can be accessed remotely.
Location-based Service	Enable or disable third-party location based services on this AP. ExtremeWireless supports the following third-party services: <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.
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 information. This option is disabled by default. If SNMP 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 ExtremeWireless <i>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.

Table 11: Multi-Edit AP Properties (continued)

Field	Description
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 when an AP model with external antennas is selected. 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 and antenna for each available port. 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 is on or off. Select On to enable the radio. Select Off to disable the radio.
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 80MHz frequency. Applies to AP38xx and AP39xx Radio 1 only. 80 MHz — Allows 802.11ac clients to use the 80MHz 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.

Table 11: Multi-Edit AP Properties (continued)

Field	Description
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 162.
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.
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 will 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 11: 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 returns both DFS and non-DFS channels, if available. All Non-DFS Channels — ACS scans all non-DFS channels for an operating channel. Custom — To configure individual channels from which the ACS will select 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. 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.
Dynamic Channel Selection	<p>Determines behavior when traffic or noise levels exceed the configured DCS thresholds. Valid values are:</p> <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	<p>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.</p>
DCS Channel Occupancy Threshold	<p>Defines the channel utilization level, measured as a percentage. If the threshold is exceeded, ACS scans for a new operating channel for the AP.</p>
DCS Update Period (Minutes)	<p>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).</p>

Table 11: Multi-Edit AP Properties (continued)

Field	Description
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.
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.

Table 11: Multi-Edit AP Properties (continued)

Field	Description
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.
Multicast to Unicast delivery	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. 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.
11n Radio Settings	
Guard Interval	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.
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.

Table 11: 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.
Extension Channel Busy Threshold	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	Determines MAC Service Data Unit (MSDU) aggregation. Enable to increase the maximum frame transmission size.
Aggregate MPDUs	Determines MAC Protocol Data Unit (MPDU) aggregation. Enable to increase the maximum frame transmission size, providing a significant improvement in throughput.
Aggregate MPDU Max Length	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.
Agg. MPDU Max # of Sub-frames	Determines the maximum number of sub frames in the aggregate MAC Protocol Data Unit (MPDU). Valid value range is 2-64.
ADDDBA Support	Block acknowledgement. Provides acknowledgement of a group of frames instead of a single frame. ADDDBA 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 and 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.

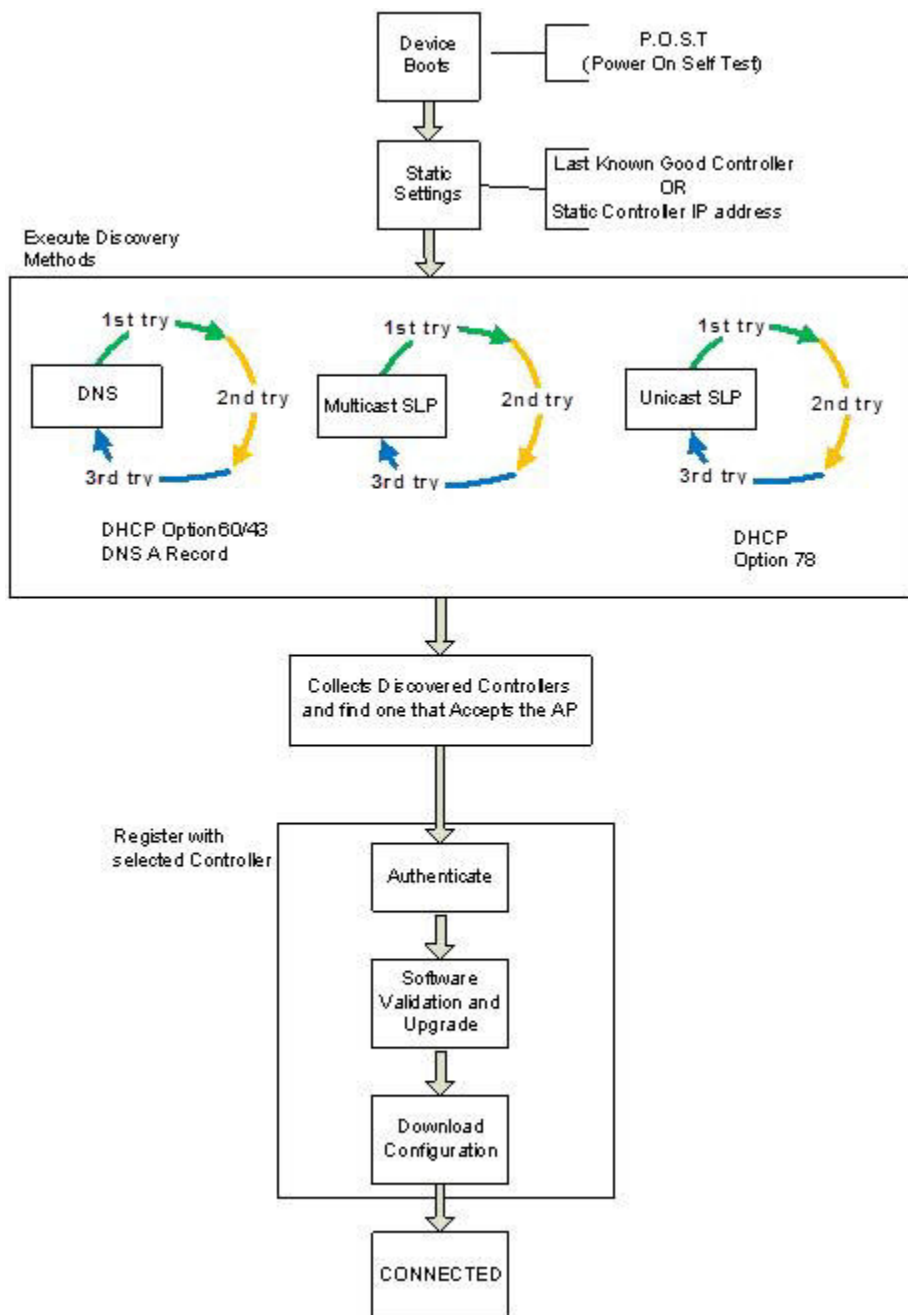


Figure 12: Wireless AP Discovery Process

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 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 122.

- **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 147.

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' configuration page. At the top, there is a navigation menu with 'Home', 'Logs', 'Reports', 'Controller', 'AP' (highlighted), 'VNS', 'Radar', and 'Help'. A 'Logout' link is in the top right. Below the menu is a search bar labeled 'Search for AP Name, Site, Model ...'. The main content is a table with the following columns: Name, Model, Site, Location, SW Version, and Status. The table contains 17 rows of AP data. Below the table, it says 'Showing: 17 rows, Local: 17'. 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"/>	0000000C29AC00AB	AP3715i		/World/Thornhill	10.11.01.0183T	Local
<input type="checkbox"/>	13310618085D0000	AP3715e			10.11.01.0183T	Local
<input type="checkbox"/>	2935	AP3825i			10.11.01.0183T	Local
<input type="checkbox"/>	3705i	AP3705i			10.11.01.0183T	Local
<input type="checkbox"/>	3801i	AP3801i			10.11.01.0183T	Local
<input type="checkbox"/>	3805	AP3805i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3825i	AP3825i			10.11.01.0183T	Local
<input type="checkbox"/>	3865e-1	AP3865e			10.11.01.0183T	Local
<input type="checkbox"/>	39350000000000e1	AP3935e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	39350000000000i1	AP3935i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3935ssdfafafa111	AP3715e			10.11.01.0183T	Local
<input type="checkbox"/>	39650000000000e1	AP3965e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	39650000000000i1	AP3965i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3965e	AP3965e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	ap3805 fcc	AP3805i-FCC			10.11.01.0183T	Local

Showing: 17 rows, Local: 17

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 checkbox for the AP and select an action from the **Actions** button. For more information, see [AP Actions](#) on page 126.
- 4 To view AP properties, click the AP row (not the checkbox). AP details are displayed.
- 5 Click **Configure** to display AP properties. For more information, see [AP Properties Tab Configuration](#) on page 150.
- 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 128.
- 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 130.

Related Links

[AP Search Facility](#) on page 125

[Understanding AP Status](#) on page 125

[AP Actions](#) on page 126

[Radio Actions](#) on page 127

[New Button -- Adding and Registering a Wireless AP](#) on page 128

[Deleting an AP](#) on page 130

[AP Properties Tab Configuration](#) on page 150

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 126

[Radio Actions](#) on page 127

[New Button -- Adding and Registering a Wireless AP](#) on page 128

[Deleting an AP](#) on page 130

[Understanding AP Status](#) on page 125

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 126.

AP Actions

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

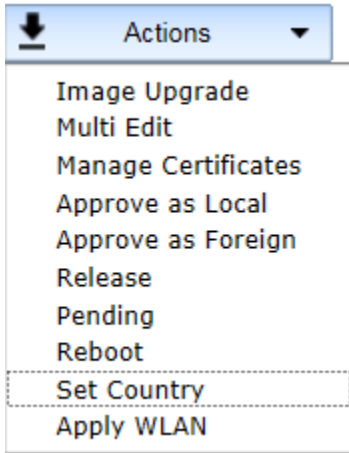


Figure 13: AP Actions button

Table 12: 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. Download appropriate image or select different APs. For information on downloading an upgrade image, see Downloading a new Wireless AP Software Image on page 203.
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 110.
Manage Certificates	Opens Certificates screen for selected APs. Configuration changes are applied to selected APs only. For more information, see Managing Certificates on page 185
Approve Local Foreign	<ul style="list-style-type: none"> Approve — a Wireless AP's status changes from Pending to Approve if the AP Registration screen was configured to register only approved APs. Approve as Local — Change a Foreign AP to a Local AP — a Wireless AP's status changes from Pending to Approve if the AP Registration screen was configured to register only approved APs. Only displays if AP rehomeing is enabled. Approve as Foreign — Change a Local AP to a Foreign AP — a Wireless AP's status changes from Pending to Approve if the AP Registration screen was configured to register only approved APs. Only displays if AP rehomeing is enabled.
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 490.
Pending	Change Status to Pending — AP is removed from the Active list, and is forced into discovery.

Table 12: AP Actions (continued)

Field	Description
Reboot	Restart selected APs without using SSH to access it.
Set Country	Select from a list of countries and apply the command to the selected APs. You are prompted to confirm your selection.
Apply WLAN	The Apply WLAN dialog appears. Select the radio for each configured WLAN Service for the selected AP. List can contain 128 WLANs. You are prompted to confirm your selection. For AP3912 only, you can select the client port for each service.

Related Links

[Modifying the Status of a Wireless AP](#) on page 147

[Assigning WLAN Services to AP3912 Ports](#) on page 159

Applying WLAN Service

Select the radio for each configured WLAN Service for the selected AP. List can contain 128 WLANs. 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 AP3912 Ports](#) on page 159

Radio Actions

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

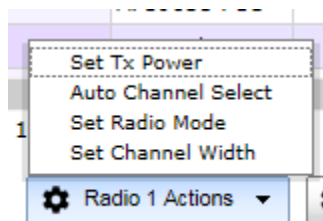
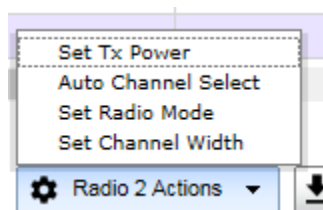
**Figure 14: Radio 1 Actions****Figure 15: Radio 2 Actions button**

Table 13: 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 165.
Auto Channel Select	Apply this command to selected APs. For more information about ACS, see Dynamic Radio Management (DRM) on page 162.
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 165.
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 165.

Related Links

[Configuration Parameters for Radio Properties](#) on page 165

[Dynamic Radio Management \(DRM\)](#) on page 162

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 147).

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 14](#) on page 129.

Clone Displays the **Clone AP** dialog. See [Creating a Clone AP](#) on page 130.

The **Add Wireless AP** screen displays.

Add Wireless AP
?
✕

Serial #:

Hardware Type: Wireless AP3825i Internal ▼

Name:

Description:

^
v

Add Wireless AP

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

Close

Table 14: 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, 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, 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, or Colombia. <p>Note: The AP37xx and AP38xx <i>cannot</i> connect to a controller licensed in the MNT domain.</p>
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.

Table 14: Add Wireless AP (continued)

Field	Description
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 147

[Creating a Clone AP](#) on page 130

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 123

[New Button -- Adding and Registering a Wireless AP](#) on page 128

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 131.
- **AP37xx W78xC**— Configure the default settings for the Radar series APs. See [Configuring AP37xx, W78xC Default AP Settings](#) on page 138.
- **AP38xx**— Configure the default settings for the ExtremeWireless Radar series APs. See [Configuring AP38xx Default AP Settings](#) on page 137.
- **AP3801**— Configure the default settings for the ExtremeWireless Radar series APs. See [Configuring AP3801 Default AP Settings](#) on page 138.
- **AP3935** — Configure the default settings for the ExtremeWireless indoor series AP. See [Configuring AP3935 Default AP Settings](#) on page 135
- **AP3965** — Configure the default settings for the ExtremeWireless outdoor series AP. See [Configuring AP3965 Default AP Settings](#) on page 136
- **AP3912** — Configure the default settings for the ExtremeWireless wall plate AP. See [Configuring AP3912 Default AP Settings](#) on page 133.

Configuring Common Configuration Default AP Settings

To configure common configuration default AP settings:

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

- In the left pane, click **Global > Default Settings**.

The **Common Configuration** tab is displayed.

Static Configuration [Hide]

Learn EWC Search List from AP

EWC Search List:

WLAN Assignments [Hide]

Associate radios:

WLAN Name	Radio 1	Radio 2	Ports
CNL-218-0-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3
CNL-218-0-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3
CNL-218-0-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3
CNL-218-0-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3
CNL-218-1-2-wds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3
CNL-218-1-4-wds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3
CNL-218-1-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3
CNL-218-1-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3



Note

Ports 1, 2, and 3, are available on the AP3912 only.

- 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 checkbox to specify a common search list for all APs. For more information about creating an EWC Search List, see [Table 18](#) on page 175.

- 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** checkbox. For more information, see [Availability](#) on page 490.
 - To associate a WLAN Service in the list to a radio and or a wired port, select the checkbox matching the radio and or port for the selected WLAN.
 - A WLAN service can be assigned to one or more radios and ports. A client port can be assigned to only one WLAN service. The assignment enables the port.
 - One policy definition for wired and wireless users. Users on wired ports receive the same default policy.
 - Wireless and wired users associated to the same WLAN service and receive identical service. They are affected by the same policies and filters.
 - ExtremeWireless v10.21.02 limits wired port assignment to open WLAN services, MBA, and captive portal.
- 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** tab.

The screenshot shows the configuration page for an AP3912 FCC. The 'AP' tab is selected in the top navigation bar. 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), Announcement Delay (2), Time To Live (120), and Country (United States). The 'Radio Settings' section is also expanded, showing settings for Radio 1 and Radio 2. The 'Advanced...' button is visible at the bottom right of the settings area, and the 'Save Settings' button is at the bottom of the page.

	Radio 1	Radio 2
Admin Mode:	On	On
Radio Mode:	a/n/ac	g/n
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 Non-DFS-Channel:	Auto

Figure 16: 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 140.

- 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** tab.

Figure 17: 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 140.

- 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:

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

The screenshot displays the configuration interface for the AP3965 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/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

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

Figure 18: 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 140.

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

Configuring AP38xx Default AP Settings

To configure AP38xx default AP settings:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.
- 3 Click the **AP38xx** 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/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 19: AP38xx Default Settings

4 Configure the following Default AP Settings as required:

- AP Properties
- Radio Settings
- Advanced Settings

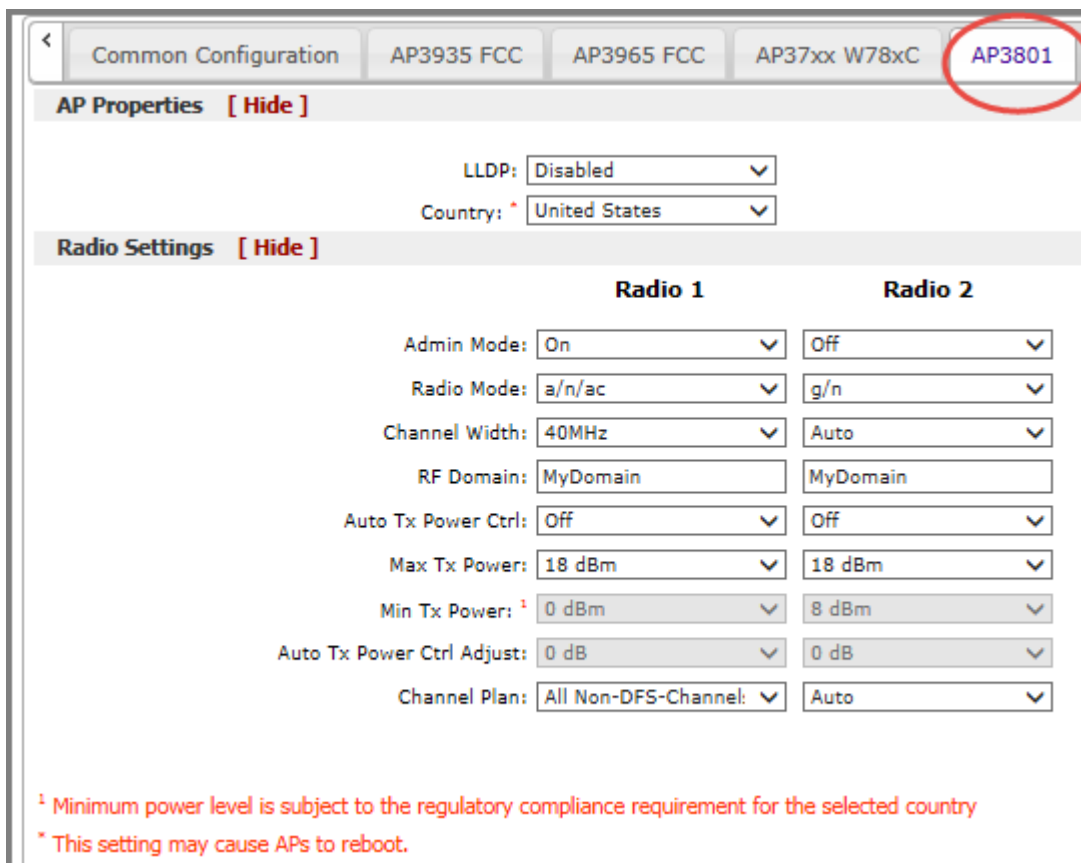
For detailed information, see [AP Default Settings](#) on page 140.

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

Configuring AP3801 Default AP Settings

To configure AP3801 default AP settings:

- From the top menu, click **AP**.
- In the left pane, click **Global > Default Settings**.
- Click the **AP3801** tab.



Common Configuration AP3935 FCC AP3965 FCC AP37xx W78xC **AP3801**

AP Properties [Hide]

LLDP: Disabled ▾
Country: * United States ▾

Radio Settings [Hide]

	Radio 1	Radio 2
Admin Mode:	On ▾	Off ▾
Radio Mode:	a/n/ac ▾	g/n ▾
Channel Width:	40MHz ▾	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 ▾

¹ Minimum power level is subject to the regulatory compliance requirement for the selected country
* This setting may cause APs to reboot.

Figure 20: AP3801 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 140.

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

Configuring AP37xx, W78xC Default AP Settings

To configure AP37xx, W78xC default AP settings:

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

- 2 In the left pane, click **Global > Default Settings**.
- 3 Click the **AP37xx W78xC** tab.

The screenshot shows the configuration interface for an AP37xx W78xC. The 'AP Properties' section includes 'LLDP: Disabled' and 'Country: United States'. The 'Radio Settings' section is split into two columns: 'Radio 1' and 'Radio 2'. The settings for Radio 1 are: Admin Mode: On, Radio Mode: a/n, Channel Width: Auto, 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, Channel Plan: All Non-DFS-Channel, and Antenna Selection: Left/Middle/Right. The settings for Radio 2 are: Admin Mode: On, 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, Channel Plan: Auto, and Antenna Selection: Left/Middle/Right. A red circle highlights the 'AP37xx W78xC' tab in the top navigation bar. A red footnote at the bottom states: '1 Minimum power level is subject to the regulatory compliance requirement for the selected country'.

Figure 21: 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 140.

- 5 Click **Save Settings**.

AP Default Settings

Table 15: AP Default Settings

Field	Description
AP Properties	
LLDP	<p>Determines if the AP broadcasts 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) — 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 <i>ExtremeWireless 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 162.</p> <p>The available radio settings are dependent on the radio mode you select.</p>

Table 15: 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 15: AP Default Settings (continued)

Field	Description
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. 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.</p>
Channel Plan	<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.</p> <p>For 5 GHz Radio nodes, click one of the following:</p> <ul style="list-style-type: none"> • All channels — ACS scans all channels for an operating channel and returns both DFS and non-DFS channels, if available. • All Non-DFS Channels — ACS scans all non-DFS channels for an operating channel. • Custom — To configure individual channels from which the ACS will select 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. <p>For 2.4 GHz Radio nodes, 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 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: 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 498.</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 15: 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 110).
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 15: 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 15: 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 15: 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 147
- [AP Properties Tab Configuration](#) on page 150
- [Setting Up the Wireless AP Using Static Configuration](#) on page 173

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 110 .

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 122

[AP Rehomng](#) on page 147

[AP Actions](#) on page 126

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.
- Model Number
- Software version running on the AP
- Country of licence.
- Number of radios
- Channel number if applicable
- Channel Mode
- Power level

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

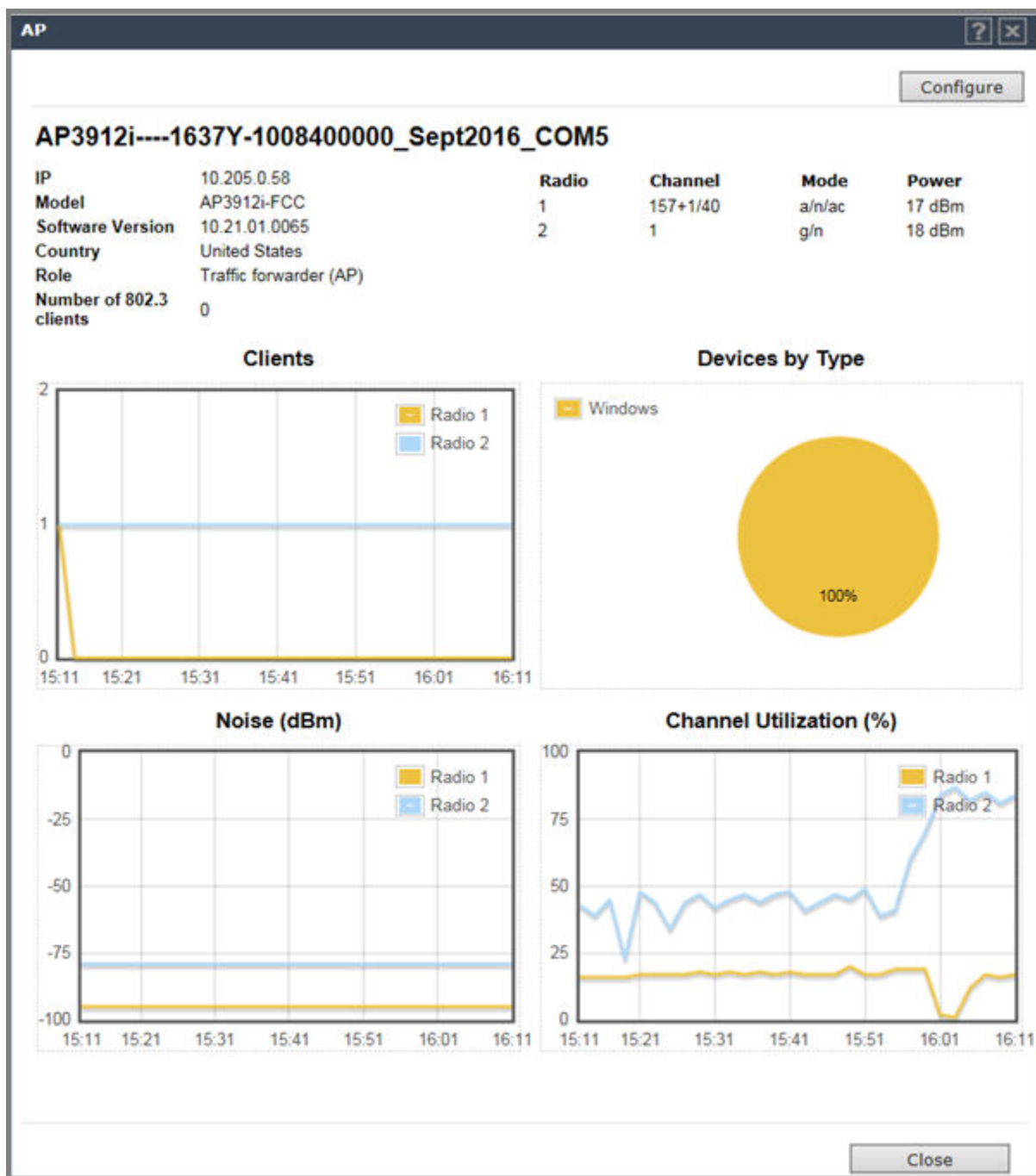


Figure 22: AP Dashboard

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 show the number of 802.3 clients. These are clients that utilize the wired client ports that are available on the AP3912.

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 150.

Related Links

[AP Properties Tab Configuration](#) on page 150

[Channel Inspector Report](#) on page 582

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 checkbox). The **AP** dashboard displays.

For more information, see [AP Dashboard](#) on page 148.

- 3 Click **Configure**. The **AP Properties** tab displays.

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.11n
Serial #:	14160242085A0000				
Host Name:	AP3825e-14160242085A0000				
Name:	C5110 - ap3 - AP3825e				
Location:	MU7 - C5110				▶
Zone:					▶
Description:	<div style="border: 1px solid gray; 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 148
- [AP Properties Tab - Basic Settings](#) on page 152
- [AP Properties Tab - Advanced Settings](#) on page 154
- [Professional Install Settings](#) on page 156
- [Assigning Wireless AP Radios to a VNS](#) on page 156
- [Configuration Parameters for Radio Properties](#) on page 165
- [Setting Up the Wireless AP Using Static Configuration](#) on page 173
- [Setting Up 802.1x Authentication for a Wireless AP](#) on page 177

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 server.
Name	Read-only. Displays the serial number of the AP.
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 557) 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. Note: The Outdoor APs can be deployed in both indoor and outdoor environments.
Hardware Type	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, and MNT. The ExtremeWireless user interface reflects the domain of the controller. The following are use cases for each domain: <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, 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, or Colombia. <p>Note: The AP37xx and AP38xx <i>cannot</i> connect to a controller licensed in the MNT domain.</p>
Application Version	Displays the ExtremeWireless release version.

Field	Description
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 147.</p>
Active Clients	<p>Displays the number of wireless devices currently associated with the AP.</p>
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 195. 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 528.</p>
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 154

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 498.</p>
Secure Tunnel	<p>This feature, when enabled, provides encryption, authentication, and key management between the AP and/or controllers. 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. If SNMP is enabled on the controller and you enable LLDP, the LLDP Confirmation dialog is displayed. 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. 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>
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 what was negotiated with the Switch PoE4). 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 572).</p>

Related Links

[AP Properties Tab - Basic Settings](#) on page 152

Professional Install Settings

The Professional Install option is only available when an AP model with external antennas is selected. 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. Choose the desired attenuation for each radio from the drop-down list. Selectable range is from 0 to 30 dBI.

Assigning Wireless AP Radios to a VNS

There are three 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 273.

**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 343.

- **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 110 .
- **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 checkbox). The **AP Details** dialog is displayed.
- 3 Click **Configure**. The **AP Properties** tab is displayed.

- 4 Click the **WLAN Assignment** tab.

WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.1x
WLAN Name	Radio 1	Radio 2		
gggWLAN	<input type="checkbox"/>	<input type="checkbox"/>		
h	<input type="checkbox"/>	<input type="checkbox"/>		
httpsWLAN	<input type="checkbox"/>	<input type="checkbox"/>		
Lab126-12-AAA	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Lab126-12-Ext-CP	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Lab126-12-Ext-CP-IA	<input type="checkbox"/>	<input type="checkbox"/>		
Lab126-12-GuestP	<input type="checkbox"/>	<input type="checkbox"/>		
Lab126-12-GuestSpl	<input type="checkbox"/>	<input type="checkbox"/>		
Lab126-12-Int-CP	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Lab126-12-Int-CP-bac	<input type="checkbox"/>	<input type="checkbox"/>		
Lab126-12-MBA	<input type="checkbox"/>	<input type="checkbox"/>		
o	<input type="checkbox"/>	<input type="checkbox"/>		
v1WLAN	<input type="checkbox"/>	<input type="checkbox"/>		
v1WLAN0	<input type="checkbox"/>	<input type="checkbox"/>		
v3WLAN	<input type="checkbox"/>	<input type="checkbox"/>		
v5WLAN	<input type="checkbox"/>	<input type="checkbox"/>		

- 5 In the **Radio 1** and **Radio 2** columns, select the AP radios that you want to assign for each WLAN Service.
- 6 To save your changes, click **Apply**.

Related Links

- [Assigning WLAN Services to AP3912 Ports](#) on page 159
- [AP Properties Tab Configuration](#) on page 150
- [Configuration Parameters for Radio Properties](#) on page 165

[Setting Up 802.1x Authentication for a Wireless AP](#) on page 177

[AP Multi-Edit Properties](#) on page 110



Assigning WLAN Services to AP3912 Ports

When configuring the AP3912, you can assign one or more client ports to a single WLAN service, but the port can only be assigned to one service. Wired ports can only be assigned to open WLAN services. There is no security or privacy on the client ports.

- 1 From the top menu, click **AP**.
- 2 Select an AP3912.
The **AP Properties** dialog appears.
- 3 Select the **WLAN Assignment** tab.

- 4 Select one or more client ports for each WLAN Service.
 - A WLAN service can be assigned to one or more radios and ports. A client port can be assigned to only one WLAN service. The assignment enables the port.
 - One policy definition for wired and wireless users. Users on wired ports receive the same default policy.
 - Wireless and wired users associated to the same WLAN service and receive identical service. They are affected by the same policies and filters.
 - ExtremeWireless v10.21.02 limits wired port assignment to open WLAN services, MBA, and captive portal.

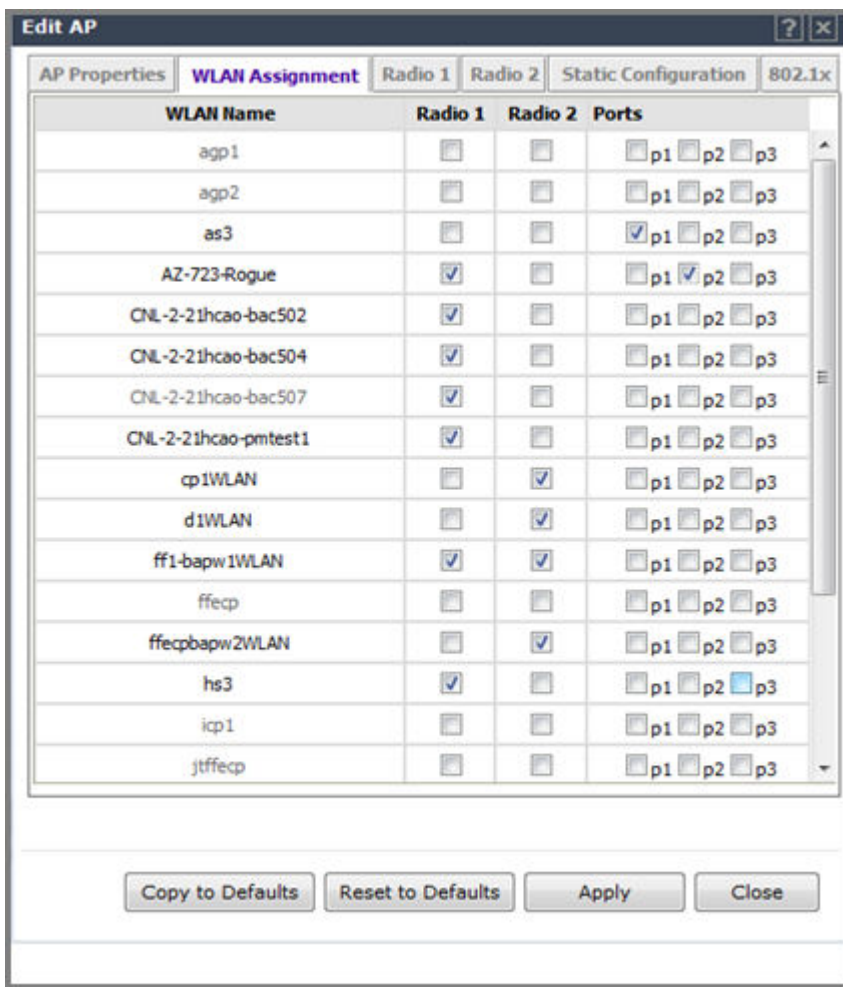


Figure 23: Assigning Ports to WLANS on the AP3912

- 5 To configure wired ports, 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. The Auto setting uses the supported values for the connected hardware in bytes per second.

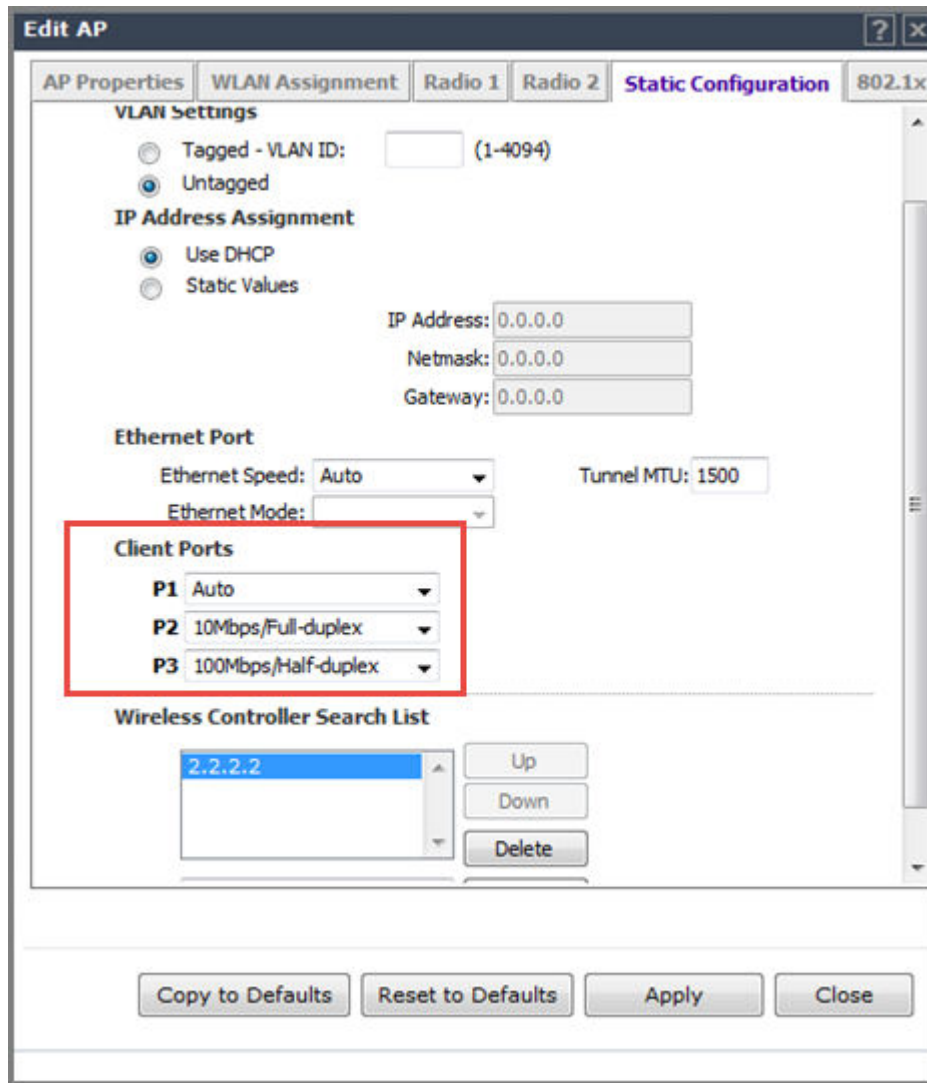


Figure 24: Port Configuration for Wired Ports

Related Links

- [AP Properties Tab - Basic Settings](#) on page 152
- [AP Properties Tab - Advanced Settings](#) on page 154
- [AP Properties Tab Configuration](#) on page 150
- [Assigning Wireless AP Radios to a VNS](#) on page 156
- [Configuration Parameters for Radio Properties](#) on page 165
- [Setting Up the Wireless AP Using Static Configuration](#) on page 173
- [Setting Up 802.1x Authentication for a Wireless AP](#) on page 177
- [Configuring Common Configuration Default AP Settings](#) on page 131

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 163.

Dynamic Radio Management (DRM)

When you modify the radio properties of an AP, the Dynamic Radio Management (DRM) functions of the controller can be used to help establish the optimum radio configuration for your APs. DRM is enabled by default. The controller's DRM:

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

The DRM feature consists of three functions:

Auto Channel Selection (ACS)

ACS provides an easy way to optimize channel arrangement based on the current situation in the field. ACS provides an optimal solution only if it is triggered on all APs in a deployment. Triggering ACS on a single AP or on a subset of APs provides a useful but suboptimal solution. Also, ACS only relies on the information observed at the time it is triggered. Once an AP has selected a channel, it remains operating on that channel until the user changes the channel or triggers ACS.

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 channel.
- **Channel Plan** — 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. Select from the following options:

Depending on the radio used, when defining a channel plan you can either create your customized channel plan by selecting individual channels or you can select a default 3 or 4 channel plan.

You can use the channel plan to avoid transmission overlap on 40 MHz channels of the wireless 802.11n APs. To avoid channel overlap between wireless 802.11n APs that operate on 40 MHz channels, configure the channel plan for the 5 GHz radio band to use every other channel available.

If using half of the available channels is not an option for your environment, do not configure a channel plan. Instead, allow ACS to select from all available channels. This alternate solution may contribute to increased congestion on the extension channels.



Note

ACS in the 2.4 GHz radio band with 40 MHz channels is not recommended due to severe co-channel interference.

Dynamic Channel Selection (DCS)

DCS allows a Wireless AP to monitor traffic and noise levels on the channel on which the AP is currently operating. DCS can operate in two modes:

- **Monitor** — When DCS is enabled in monitor mode and traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. The DCS monitor alarm is used for evaluating the RF environment of your deployed APs.
- **Active** — When DCS is enabled in active mode and traffic or noise levels exceed the configured DCS thresholds, 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 select an alternate channel for the AP to operate on. DCS does not trigger channel changes on neighboring APs.



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 566.

Auto Tx Power Control (ATPC)

ATPC guarantees your LAN a stable RF environment by automatically adapting transmission power signals according to the coverage provided by the APs. ATPC can be either enabled or disabled.

When you disable ATPC, you are given the option of automatically adjusting the Max Tx Power setting to match the Current Tx Power Level. In the case of AP Multi-edit, if you reply yes, then each individual AP's Max Tx Power setting is adjusted to correspond with its Current Tx Power Level in the database.

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 checkbox). 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 16: 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.ac strict capability. • n-strict – Click to enable the 802.11a mode of Radio 1 with 802.11n strict capability.

Table 16: 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 162).
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>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, see Regulatory Information on page 650.</p>

Table 16: 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 16: 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 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"> • All channels — ACS scans all channels for an operating channel and returns both DFS and non-DFS channels, if available. • All Non-DFS Channels — ACS scans all non-DFS channels for an operating channel. This selection is always available, but if there are no DFS Channels available, the list is the same as the All Channels list. • 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.
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 169

[Radio Actions](#) on page 127

[AP Properties Tab Configuration](#) on page 150

[Assigning Wireless AP Radios to a VNS](#) on page 156

[Setting Up the Wireless AP Using Static Configuration](#) on page 173

[Setting Up 802.1x Authentication for a Wireless AP](#) on page 177

Radio Advanced Properties

Table 17: 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.
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. For the AP38xx, this setting is only available on Radio 2. This setting is not applicable on either radio for the AP39xx. 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.

Table 17: Advanced Radio Properties (continued)

Field	Description
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.
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.

Table 17: Advanced Radio Properties (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 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	
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 checkbox). 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.

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 . 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 checkbox). 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 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 177. 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

	Up
	Down
	Delete
	Add



Note

Client Port configuration is available for the AP3912. For more information, see [Assigning WLAN Services to AP3912 Ports](#) on page 159.

Table 18: 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 18: 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 52). 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 119.
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 18: 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 150

[Assigning Wireless AP Radios to a VNS](#) on page 156

[Configuration Parameters for Radio Properties](#) on page 165

[Setting Up 802.1x Authentication for a Wireless AP](#) on page 177

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 150

[Assigning Wireless AP Radios to a VNS](#) on page 156

[Configuration Parameters for Radio Properties](#) on page 165

[Setting Up the Wireless AP Using Static Configuration](#) on page 173

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 179
- [Pass Through Mode](#) on page 181



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 checkbox) 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 19](#) on page 187 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 checkbox). 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 checkbox) 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 a window titled "Extreme networks Wireless AP Credentials". The window is divided into two main sections: "Current credentials in use by Wireless AP" and "EAP-TLS Certificate".

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=testvpc, DC=com

Full subject distinguished name: CN=Users, CN=AP1Credential, DC=com,

Subject alternative name: Principal Name=ap_admin

At the bottom of the window is a "Close" button.

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 checkbox) 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 menu with tabs: Home, Logs, Reports, Controller, **AP** (selected), VNS, Radar, and Help. A Logout link is visible in the top right corner. Below the menu is a search bar labeled "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 17 APs, all with a status of "Local". Below the table, it says "Showing: 17 rows, Local: 17". 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"/>	0000000C29AC00AB	AP3715i		/World/Thornhill	10.11.01.0183T	Local
<input type="checkbox"/>	13310618085D0000	AP3715e			10.11.01.0183T	Local
<input type="checkbox"/>	2935	AP3825i			10.11.01.0183T	Local
<input type="checkbox"/>	3705i	AP3705i			10.11.01.0183T	Local
<input type="checkbox"/>	3801i	AP3801i			10.11.01.0183T	Local
<input type="checkbox"/>	3805	AP3805i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3825i	AP3825i			10.11.01.0183T	Local
<input type="checkbox"/>	3865e-1	AP3865e			10.11.01.0183T	Local
<input type="checkbox"/>	39350000000000e1	AP3935e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	39350000000000i1	AP3935i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3935ssdfafafa111	AP3715e			10.11.01.0183T	Local
<input type="checkbox"/>	39650000000000e1	AP3965e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	39650000000000i1	AP3965i-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	3965e	AP3965e-FCC			10.11.01.0183T	Local
<input type="checkbox"/>	ap3805 fcc	AP3805i-FCC			10.11.01.0183T	Local

- 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 19](#) on page 187 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.

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 19](#) on page 187 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 19: 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.
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 183

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. The following table lists the maximum number of load balance groups for each controller.

Table 20: Maximum Number of Load Balance Groups

ExtremeWireless Appliance	Number of load balance groups
C4110	32
C5110	64
C5210	64
C25	8
C35	8
V2110	64
V2110H	64

Currently, the following wireless AP models support load balance groups:

- AP39xx
- AP3801i
- AP3805 (i & e)
- AP3825 (i & e)
- AP3865e
- AP3765/67
- AP3705i
- AP3710 (i & e)
- AP3715 (i & e)

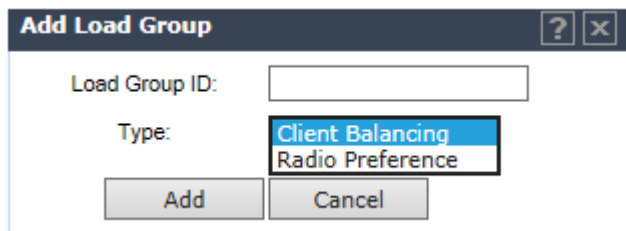
To create a load balance group, see [Creating a Load Balance Group](#) on page 188.

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></th> <th>Enable</th> <th>Max # of Clients</th> <th>Strict Limit</th> </tr> </thead> <tbody> <tr> <td>Radio1</td> <td><input type="checkbox"/></td> <td><input type="text" value="112"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Radio2</td> <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	Radio1	<input type="checkbox"/>	<input type="text" value="112"/>	<input type="checkbox"/>	Radio2	<input type="checkbox"/>	<input type="text" value="112"/>	<input type="checkbox"/>
	Enable	Max # of Clients	Strict Limit											
Radio1	<input type="checkbox"/>	<input type="text" value="112"/>	<input type="checkbox"/>											
Radio2	<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"/>												
39350000000000e1*(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	
<i>gggWLAN</i>	<input type="checkbox"/>
<i>h</i>	<input type="checkbox"/>
<i>httpsWLAN</i>	<input type="checkbox"/>
<i>Lab126-12-AAA</i>	<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"/>
<i>Lab126-12-MBA</i>	<input type="checkbox"/>
<i>o</i>	<input type="checkbox"/>
<i>v1WLAN</i>	<input type="checkbox"/>
<i>v1WLAND</i>	<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 191.

Configuration Parameters for AP Load Groups

Table 21: 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 WLANs assigned to the group. Radio Preference - select to perform band preference steering and enforce load control settings on this load group.

Table 21: 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 checkbox 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 checkbox 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 checkbox 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 21: AP Load Groups (continued)

Field/Button	Description
WLAN Assignment tab	
WLAN Name	Click the checkbox 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 checkbox 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 492.

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 576.

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 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** checkbox. 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** checkbox.
- 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.



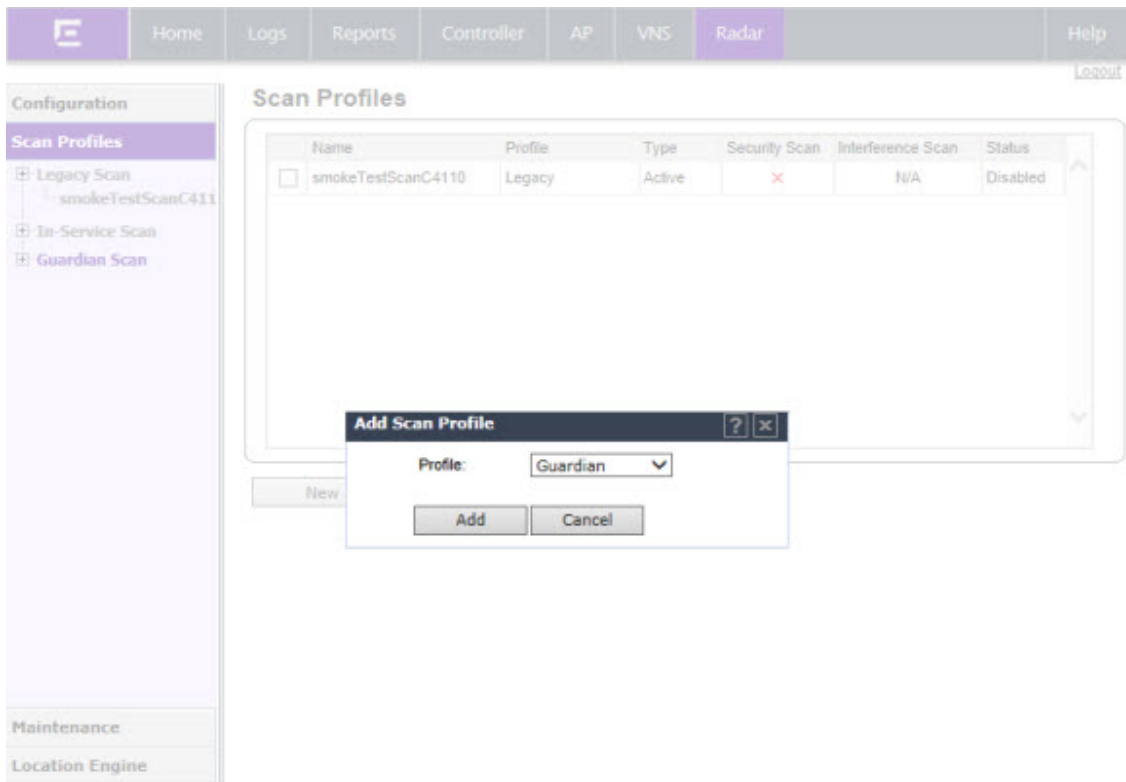
Note

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 **Radar**. The **Radar** screen displays.
- In the left pane, expand **Scan Profiles**. The **Scan Profiles** screen displays.

- 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 528.

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; however, mobile user roaming is not supported with central RADIUS authentication.

The IPv4 address pool used by un-authenticated clients must be large enough to provide additional IP addresses to all APs configured with Firewall Friendly External Captive Portal (ECP). This is because each AP creates a virtual interface on each non-authenticated policy VLAN and assigns an IP address to it from the pool.

To configure an External Captive Portal on an AP, the following is required:

- The WLANS 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.

Related Links

[Configuring Firewall Friendly External Captive Portal on an AP](#) on page 197

[Controlling Network Access on the AP](#) on page 199

[Configuring Firewall Friendly External Captive Portal](#) on page 306

[Assigning RADIUS Servers for Authentication](#) on page 293

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 224.

If using RADIUS authentication, FF-ECP on the AP can work with both local and central RADIUS authentication. The AP must be in Site mode.

- 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.

Role: Allow_VLAN

VLAN & Class of Service

Core

Role Name: Allow_VLAN

Default Action

Access Control: None
No change
Allow
Deny
Containment VLAN

Default Class of Service: None

Traffic Mirror: 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.

The Allow and Containment VLAN options with the B@AP topology redirects HTTP traffic on the AP. For B@AP traffic, only the FF ECP is supported as an external captive portal.



Note

FFECP @AP is dependent on the configured non-authenticated VLAN ID. Do not change the client's VLAN ID at runtime.

On the Policy Rules tab, enable **AP Filtering**.

Role: Allow_VLAN

VLAN & Class of Service | **Policy Rules**

Inherit filter rules from currently applied role ⓘ

Rules AP Filtering Custom AP Rules

Configure specific policy filters.

- Allow and DNS traffic.
- Mobile user access to FF-ECP.
- Mobile user access to AP.
- HTTP(S) redirection.

For more information, see [Configuring Rule-Based Redirection](#) on page 246.

- 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 293.
 - 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 **FFECP Configure** dialog.
 - Select the Vendor Specific Attributes (VSAs) for authentication. For more information, see [Vendor Specific Attributes](#) on page 297.
 - Select an option for **Send Successful Login To**.

For FFECP 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 224
- [Configuring Rule-Based Redirection](#) on page 246
- [Understanding the Filter Rule Definition Dialog](#) on page 257
- [Configuring a Basic WLAN Service](#) on page 274
- [Configuring WLAN Service Privacy](#) on page 285
- [Configuring Firewall Friendly External Captive Portal](#) on page 306
- [Assigning RADIUS Servers for Authentication](#) on page 293

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 257.

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**.

- In the left pane, click **Global > Maintenance**.

The following screen appears:

The screenshot shows the 'AP Software Maintenance' configuration interface. It is divided into two main sections: 'AP Images for Platform' and 'Download AP Images:'.
 In the 'AP Images for Platform' section, a dropdown menu is set to 'AP3705i'. Below it, a list of images is shown, with 'AP3705-10.11.01.0190T.img (Default)' selected. There are 'Set as default' and 'Delete' buttons below the list.
 The 'Download AP Images:' section contains several input fields: 'FTP Server', 'User ID', 'Password', 'Confirm', 'Directory', 'Filename', and 'Platform' (set to 'AP3705i'). A 'Download' button is located at the bottom right of this section.
 Below these sections is the 'Upgrade Behavior:' section, which has two radio button options: 'Upgrade when AP connects using settings from Controlled Upgrade' (unselected) and 'Always upgrade AP to default image (overrides Controlled Upgrade settings)' (selected).
 At the bottom of the page, it displays 'Disk space left for images: 13019 MB' and a 'Save' button.

- In the **AP Images for Platform** drop-down list, click the appropriate platform.
- To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.
- 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.
- To save your changes, click **Save**.

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:

The screenshot shows the 'AP Maintenance Cycle' configuration interface. It is divided into three main sections:

- Schedule:** Includes a 'Start At' field set to '00:00' and a 'Duration' dropdown menu currently set to '3 hours'.
- Recurrence:** Features a group of radio buttons for selecting the frequency: 'Never', 'Daily' (selected), 'Weekly', 'Monthly', 'Every day' (selected), 'Every weekday', and 'Every weekend'.
- Platforms:** A grid of checkboxes for selecting specific AP models. The checked models are AP3705 and AP3715. Other models listed include AP3710, AP3765, AP3767, AP3801, AP3805, AP3825, AP3865, AP3935, AP3965, APVMAP, W78XC, and W78XCSPF.

A 'Save' button is located at the bottom right of the configuration area.

- 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.

AP Software Maintenance
Controlled Upgrade

Step 1: Select AP Platform:

Step 2: Select an image to use:

Step 3: Apply the AP image from Step 2 to the selected APs below:

	Wireless APs	Current version	Upgrade to
<input type="checkbox"/>	3705i	10.11.01.0190T	

Step 4: Repeat Steps 1 - 3 as necessary

Step 5: Save this upgrade strategy for later, or upgrade the APs now:



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 checkbox 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 checkbox on the **AP Software Maintenance** tab overrides the Controlled Upgrade settings.

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 208
- [37xx Series Wireless APs](#) on page 212

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 216.

39xx Series Wireless APs



AP3912 LED Indicators

The AP3912i has six LED indicators. The LEDs provide status information on the current state of the AP3912i.

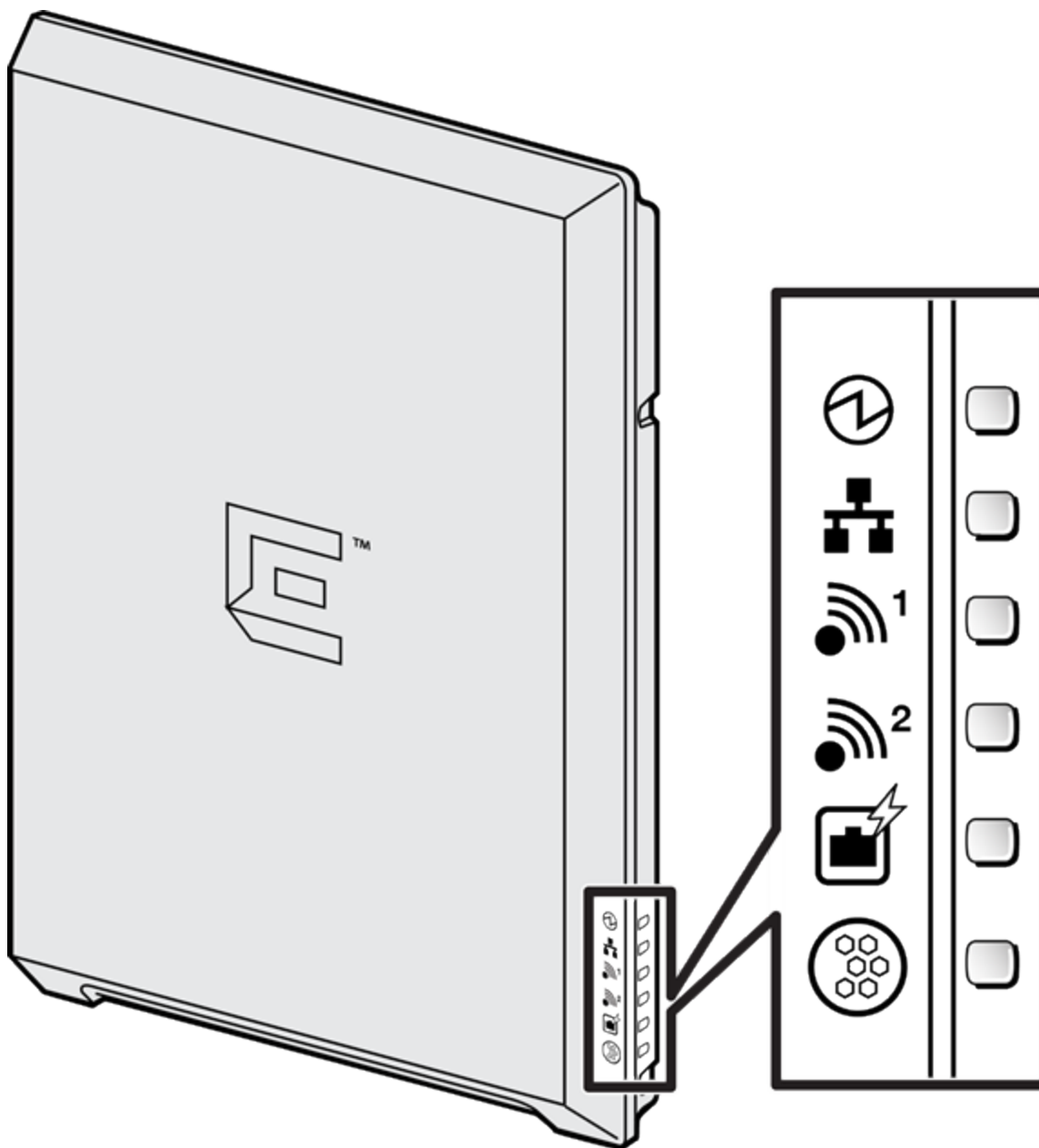


Figure 25: AP3912i LEDs

Table 22: AP3912i LED Status Indicators







LED	Indicator	Status	Description
1 (Status)		Green	Indicates AP is working normally
		Amber	System failure
2 (Ethernet link state) LAN 1		Amber	Indicates a valid 1Gbps Ethernet link
		Green	Indicates a valid 10Mbps or 100Mbps Ethernet link

Table 22: AP3912i LED Status Indicators (continued)

LED	Indicator	Status	Description
3 (Radio 1)	 1	Green	Indicates Radio 1 is enabled
4 (Radio 2)	 2	Green	Indicates Radio 2 is enabled
5 (PSE Client Port)		Green	Uplink AP port detects AF PoE source
6 (BLE)		Green	Indicates BLE is enabled

AP3935, AP3965 LED Indicators

The AP3935 and AP3965 provide 5 LED indicators. The LEDs provide status information on the current state of the AP.

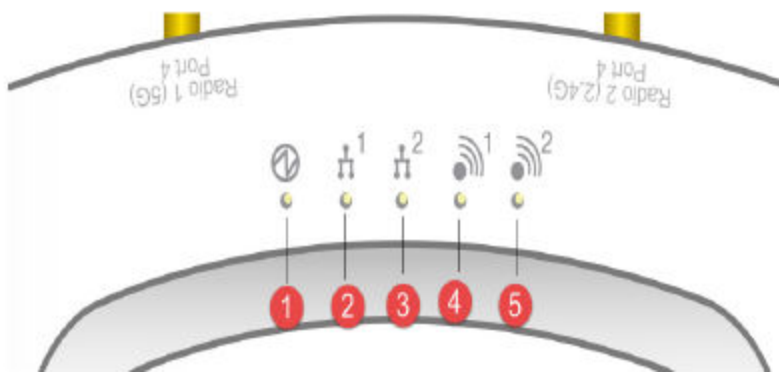


Table 23: LED Indications AP3935 and AP3965

LED	Status	Description
1 (AP status)	On Green	Indicates that the AP is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Amber	Indicates a CPU/system failure.
2 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.

Table 23: LED Indications AP3935 and AP3965 (continued)

LED	Status	Description
	Off	Indicates the link is down.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Radio 1 (5 GHz) status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.
5 (Radio 2 (2.4 GHz) status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.

38xx Series Wireless APs

WS-AP3801i LED Indicators

The WS-AP3801i provides three LED indicators. Refer to [the following figure](#). The LEDs provide status information on the current state of the WS-AP3801i. Refer to [the following table](#).

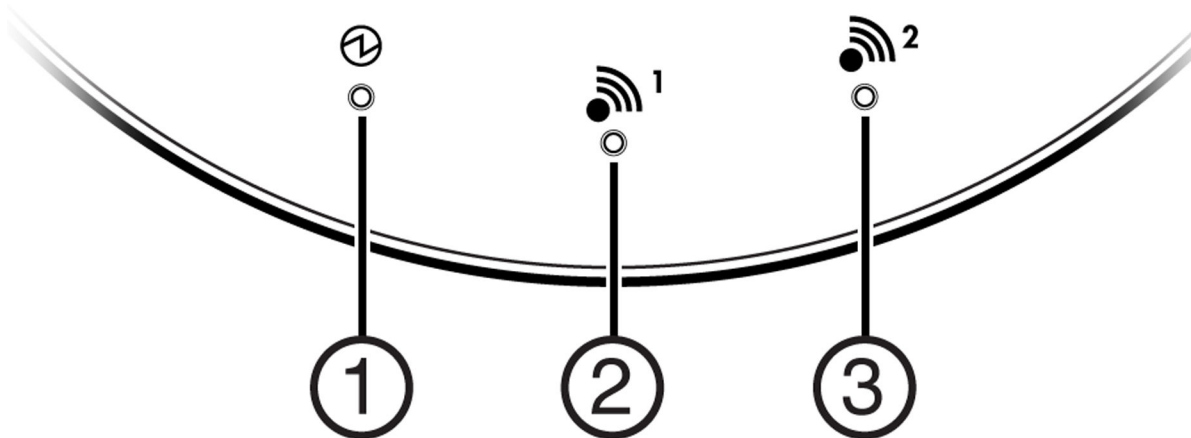


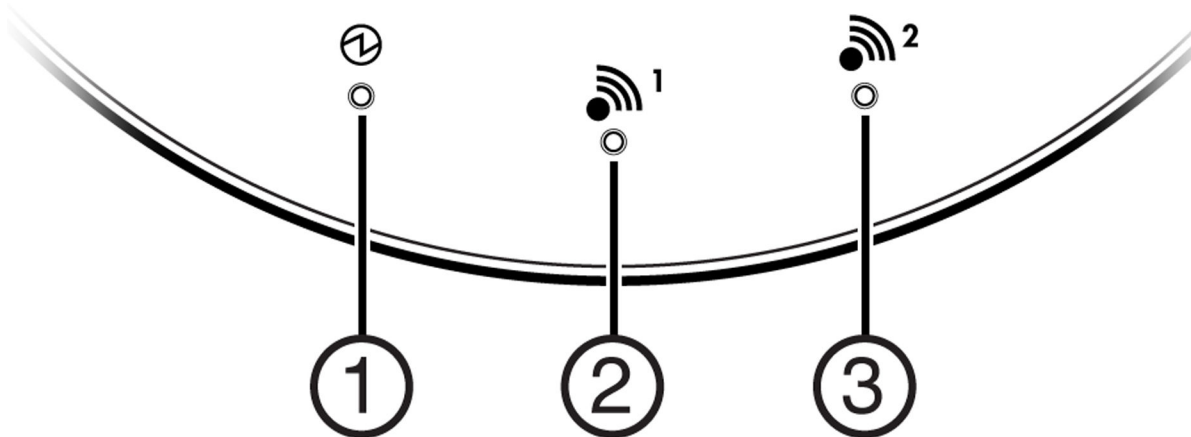
Figure 26: AP3801i Top View

Table 24: AP3801i LED Status Indicators

LED	Status	Description
1 (Power)	On Green	Indicates the AP3801 is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Red	Indicates a CPU or system failure.
2 (Radio 1 Status)	On Green	Indicates Radio 1 (5.0 GHz) is enabled.
3 (Radio 2 Status))	On Green	Indicates Radio 2 (2.4 GHz) is enabled.

WS-AP3805i/e LED Indicators

The WS-AP3805i/e provides three LED indicators (see [Figure 27](#)). The LEDs provide status information (see [Table 25](#)) on the current state of the WS-AP3805i/e.

**Figure 27: AP3805i/e Top View****Table 25: AP3805i/e LED Status Indicators**

LED	Status	Description
1 (Power)	On Green	Indicates the AP3805 is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Red	Indicates a CPU or system failure.

Table 25: AP3805i/e LED Status Indicators (continued)

LED	Status	Description
2 (Radio 1 Status)	On Green	Indicates Radio 1 (5.0 GHz) is enabled.
3 (Radio 2 Status)	On Green	Indicates Radio 2 (2.4 GHz) is enabled.

WS-AP3865 LED Indicators

The WS-AP3865e has five LED indicators, as shown in [the figure below](#). The LEDs provide status information, described in [Table 26](#), on the current state of the WS-AP3865e.

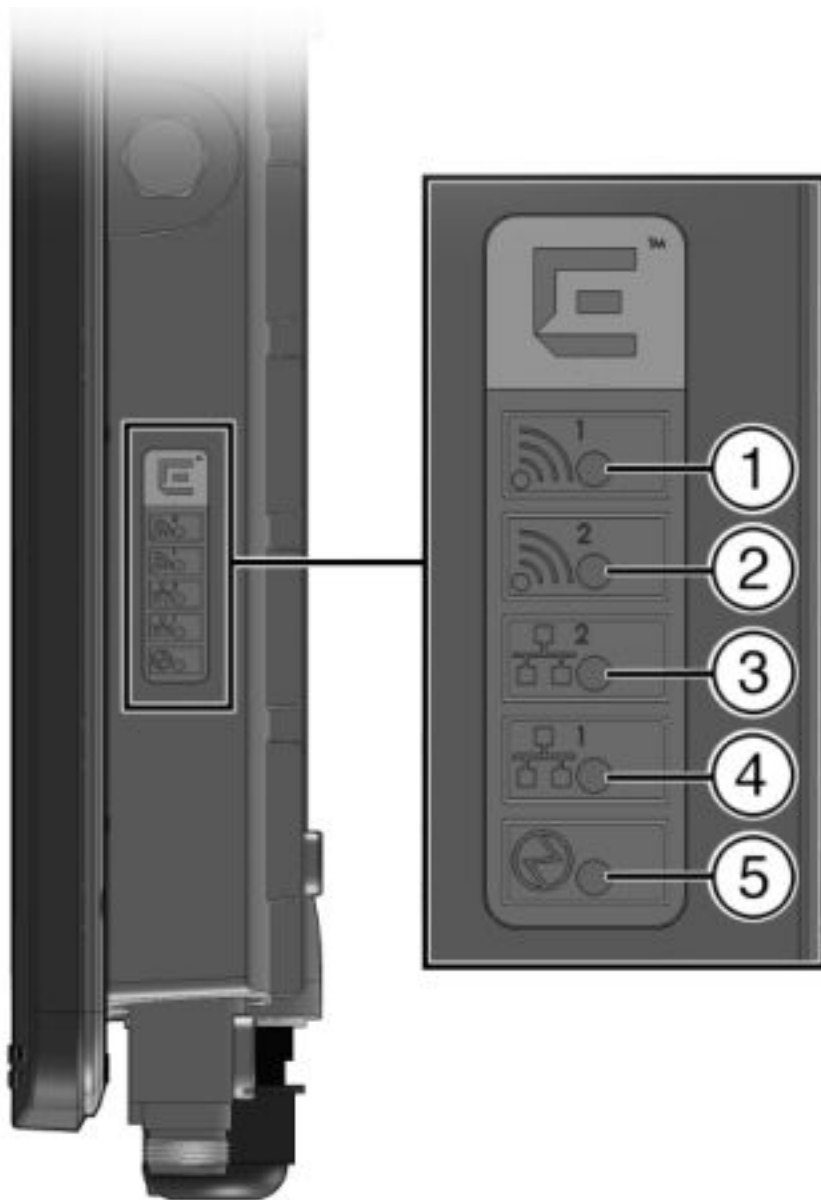


Figure 28: WS-AP3865e LEDs

Table 26: WS-AP3865 LED Indications

LED	Status	Description
1 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.
2 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
5 (AP status)	On Green	Indicates the WS-AP3865 is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Amber	Indicates a CPU/system failure.

WS-AP3825 LED Indicators

The WS-AP3825 has five LED indicators, as shown in [the figure below](#). The LEDs provide status information, described in [Table 27](#), on the current state of the WS-AP3825.

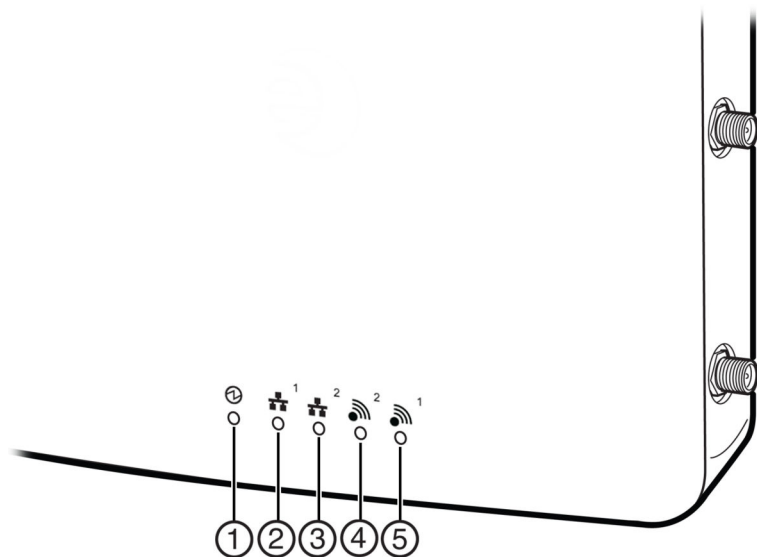


Figure 29: WS-AP3825 LEDs

Table 27: WS-AP3825 LED Indications

LED	Status	Description
1 (AP status)	On Green	Indicates the WS-AP3825 is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Amber	Indicates a CPU/system failure.
2 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.
5 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.

37xx Series Wireless APs

The ExtremeWireless AP37xx series are 802.11n APs, with added capacity for intrusion threat detection and prevention capability. The LED indicators on these are described in the following subsections:

- [WS-AP3710 LED Indicators](#) on page 213
- [WS-AP3715 LED Indicators](#) on page 214
- [AP3765/AP3767/W786C LED Status](#) on page 216

WS-AP3705i LED Indicators

The WS-AP3705i provides four LED indicators (see [the following figure](#)). The LEDs provide status information (see [Table 28](#)) on the current state of the WS-AP3705i.

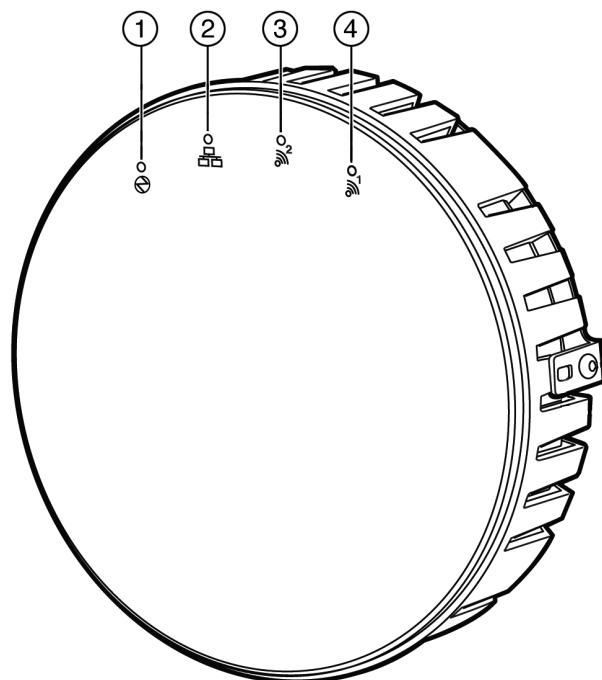


Figure 30: AP3705i Top View

Table 28: AP3705i LED Status Indicators

LED	Status	Description
1 (Power)	On Green	Indicates the AP3705 is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Red	Indicates a CPU or system failure.
2 (Ethernet Link)	On Blue	Indicates a valid 1Gbps Ethernet link.
	On Green	Indicates a valid 100Mbps Ethernet link.
	Off	Indicates the link is down.
3 (Radio 2 Status)	On Green	Indicates Radio 2 (2.4 GHz) is enabled.
4 (Radio 1 Status)	On Green	Indicates Radio 1 (5 GHz) is enabled.

WS-AP3710 LED Indicators

Both models (AP3710i and AP3710e) of the WS-AP3710 have four LED indicators, shown in [the figure below](#). The LEDs provide status information, described in [Table 29](#) on page 214, on the current state of the WS-AP3710.

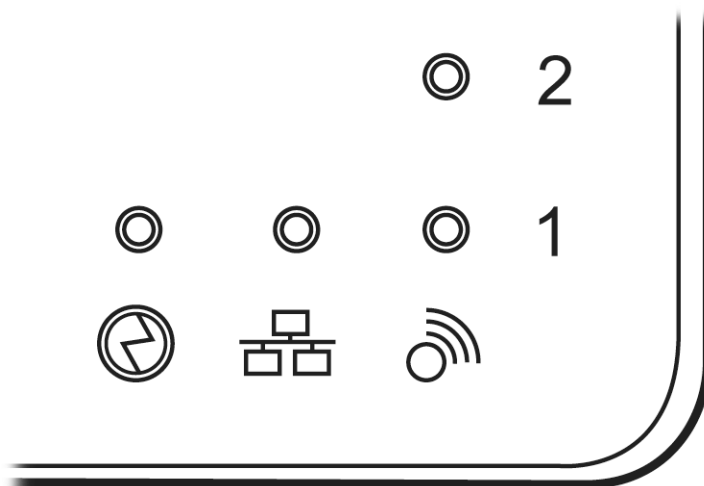


Figure 31: WS-AP3710 LEDs (Front, lower right)

 Identifies Power Indicator LED	 Identifies LAN Indicator LED	 Identifies Radio Indicator LEDs
---	---	--

Table 29: WS-AP3710 LED Indications

LED	Status	Description
1 (AP status)	On Green	Indicates the WS-AP3710 is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Red	Indicates a CPU/system failure.
2 (Ethernet link state)	On Green	Indicates a valid 100Mbps Ethernet link.
	On Blue	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
3 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
4 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.

WS-AP3715 LED Indicators

The WS-AP3715 has six LED indicators, as shown in [the figure below](#). The LEDs provide status information, described in [Table 30](#) on page 215, on the current state of the WS-AP3715.

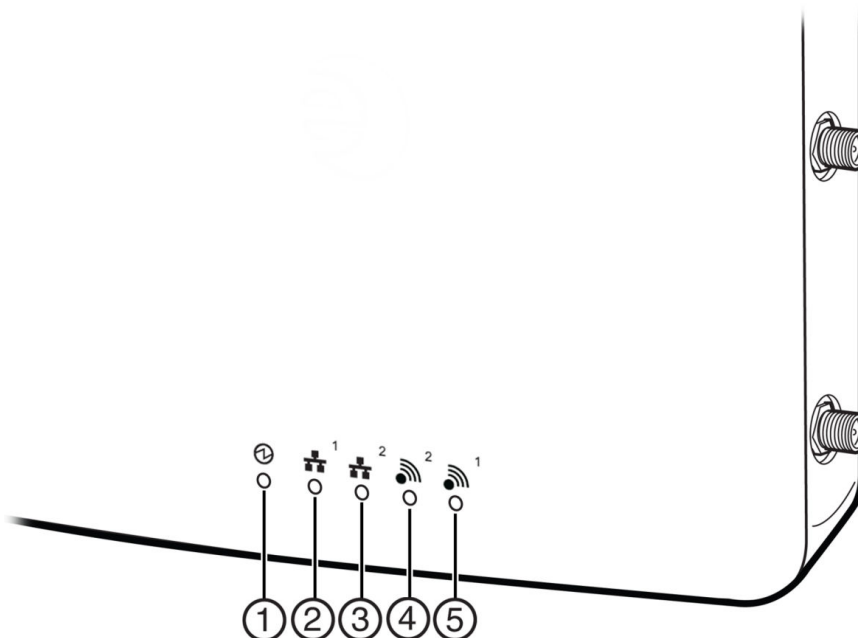


Figure 32: WS-AP3715 LEDs




 Identifies Power Indicator LED	 Identifies LAN Indicator LED	 Identifies Radio Indicator LEDs
---	---	--

Table 30: WS-AP3715 LED Indications

LED	Status	Description
1 (AP status)	On Green	Indicates the WS-AP3825 is working normally.
	Flashing Green	Indicates: <ul style="list-style-type: none"> • running a self test • loading software program
	On Amber	Indicates a CPU/system failure.
2 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.
5 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.

AP3765/AP3767/W786C LED Status

The ExtremeWireless AP3765i, W786C, AP3765e, and AP3767e models are nearly identical in appearance (e models have external antenna ports). LED status indicator displays are the same on all three models. The frontal view of the housing cover (see the following figure) displays six LEDs. These LEDs provide information on operating status.

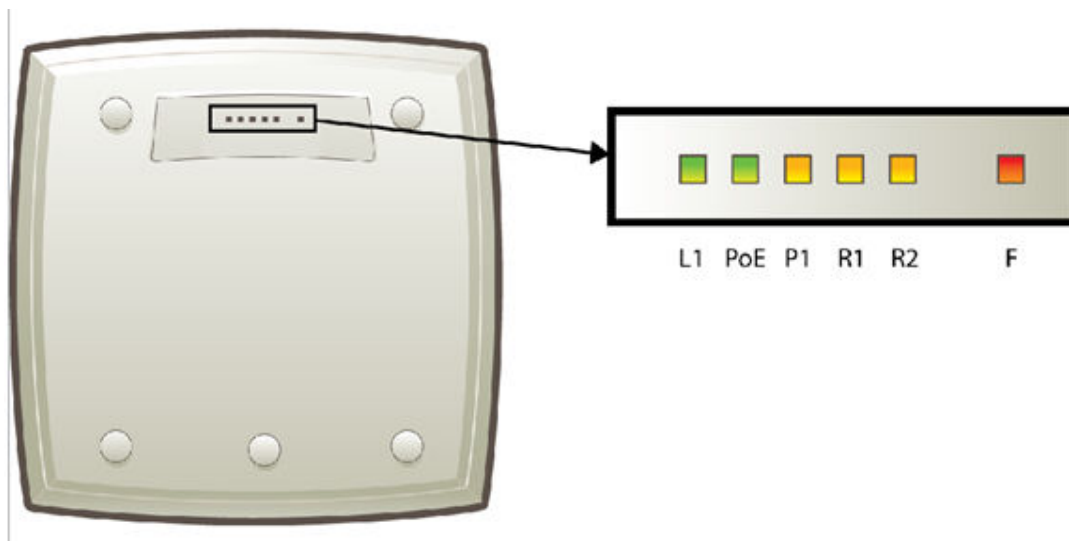


Figure 33: Wireless Outdoor AP3765/AP3767/W786C LEDs

Table 31: AP3765/AP3767 LED Status Indicators

LED	Color	Meaning
L1	Green	Power LED. When on, indicates AP power is sourced from power supply.
PoE	Green	PoE power LED. When on, indicates AP power is sourced from PoE.
P1	Green	Ethernet port 1 LED. When green on, indicates Ethernet port activity. When off, Ethernet is off, WDS is enabled.
R1	Green	WLAN Radio 1 LED. When green on, indicates Radio 1 is active.
R2	Green	WLAN Radio 2 LED When green on, indicates Radio 2 is active.
F	Red	Error LED. When on, indicates error. When off, indicates normal operation, AP connected to controller.

Configuring Wireless AP LED Behavior

You can configure the behavior of the LEDs so that they provide the following information:

Table 32: LED Operational Modes

LED Mode	Information Displayed
Off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
Normal	Identifies the AP status during the registration process during power on and boot process.
Identify	All LEDs blink simultaneously approximately two to four times every second.

You can configure the AP LED mode when you configure the following:

- An individual AP.
- Multiple APs simultaneously.
- Default AP behavior.

**Note**

You can configure all four AP LED modes if you configure an individual AP or multiple APs simultaneously. If you configure the default AP behavior, the only LED modes available are Off and Normal.

Related Links

[AP Multi-Edit Properties](#) on page 110

[AP Properties Tab - Advanced Settings](#) on page 154

Configuring Operational Mode for One AP

To configure the AP LED operational mode when configuring an individual wireless AP:

- 1 From the top menu, click **AP > APs**.
- 2 In the AP list, click a wireless AP (not the checkbox).
The **AP Configuration** page displays with the **AP Properties** tab exposed.
- 3 On the **AP Properties** tab, click **Advanced**.
- 4 In the **LED** field, select an LED operational mode.
See [Table 32](#) on page 217 for a description of each option.

Configuring Operational Mode with Multi-Edit

To set the AP LED Operational Mode when using the AP Multi-edit feature:

- 1 From the top menu, click **AP**.
- 2 Select the checkbox for more than one AP.
- 3 Click **Actions > Multi Edit**.
The **Multi Edit** dialog displays.
- 4 In the LED field, select an LED operational mode.
See [Table 32](#) on page 217 for a description of each option.

Configuring AP Operational Mode Default Behavior

To set the AP LED Operational Mode when configuring default AP behavior:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.
- 3 Click the AP tab that corresponds to the type of AP that you want to configure.
- 4 Click **Advanced**. The **Advanced** window displays.

In the LED field, select an LED operational mode. See [Table 32](#) on page 217 for a description of each option.

5 Configuring Topologies

Topology Overview
Configuring the Admin Port
Configuring a Basic Data Port Topology
Creating a Topology Group
Edit or Delete a Topology Group
Enabling Management Traffic
Layer 3 Configuration
Exception Filtering
Multicast Filtering

Topology Overview

A topology can be thought of as a VLAN with at least one egress port, and optionally, sets of services, exception filters and multicast filters.

ExtremeWireless makes use of a number of different topology modes:

- Admin - This is the topology to which the management plane's administration interface is assigned. It is the only topology that can be assigned to the administration interface. The interface must be present at layer 3 to receive management related traffic such as ssh, https and RADIUS. This interface supports IPv4 and IPv6.
- Physical - A physical mode topology is intended to be used for management purposes. A physical topology can also be used to carry station traffic for a "3rd party VNS", a VNS that uses non-Extreme Networks wireless APs. A physical topology can be assigned to any of the data plane ports on the controller.
- Routed - For this type of topology the controller acts as a router between the topology's VLAN and the rest of the network. The controller's data plane ports can be assigned to this type of topology.
- Bridged Traffic Locally at EWC - For this type of topology the controller bridges traffic for the station through its interfaces, rather than routing the traffic. For this type of topology the station's "point of presence" on the wired network is the data plane port assigned to the topology.
- Bridged Traffic Locally at AP - This type of topology is assigned to APs. For this type of topology the AP bridges traffic between its wired and wireless interfaces without involving the controller. The station's "point of presence" on the wired network for a bridged at AP topology is the AP's wired port.



Note

IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.

Define the following parameters on the **Topologies** configuration page:

- VLAN ID and associated L2 port
- L3 (IP) interface presence and the associated IP address and subnet range

- The rules for using
- Enabling or disabling the use of the associated interface for management/control traffic
- Selection of an interface for AP registration
- Multicast filter definition
- Exception filter definition

The controller has two types of Layer 2 ports:

- Admin - which can only be used for management-related purposes. It is connected directly on the management plane of the controller.
- Physical - which can be used for a variety of purposes, including bridging and routing as well as management. The physical ports are directly connected to the controller's data plane, although traffic received at physical ports may be sent up the exception path to the management plane.

At most, one physical topology can be enabled for the multicast support for Routed VNS. This can be configured on the new physical port GUI. For more information, see [Configuring the Admin Port](#) on page 220.

Configuring the Admin Port

The Admin port is a physical ethernet port directly connected to the controller's management plane. It provides a dedicated connection to a secure management VLAN. The controller can use the Admin port to interact with RADIUS, SNMP, and Extreme Management Center servers.

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

2 In the left pane, click **Network** > **Topologies**. The **Topologies** tab is displayed.

The screenshot displays the 'Topologies' configuration page. The left sidebar shows a navigation menu with 'Network' selected, and 'Topologies' highlighted. The main content area contains a table of topology configurations. Below the table are buttons for 'New' and 'Delete Selected', and a form for 'Internal VLAN ID' and 'Multicast Support'. A 'Save' button is located at the bottom right of the configuration area.

Topology Name	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	-	×	Admin	Static: 192.168.14.11 Dynamic IP Address	Admin
<input type="checkbox"/> Bridged at AP untagged	4093	×	-	-	B@AP
<input type="checkbox"/> CNL-422-0-0	4090	×	-	10.219.44.1	Routed
<input type="checkbox"/> CNL-422-0-1	4089	×	-	10.219.44.9	Routed
<input type="checkbox"/> CNL-422-0-2	42	✓	Port2	10.219.42.1	B@EWC
<input type="checkbox"/> CNL-422-0-3	4088	×	-	10.219.44.25	Routed
<input type="checkbox"/> CNL-422-1-2-wds	4087	×	-	-	B@AP
<input type="checkbox"/> CNL-422-1-4-wds	4086	×	-	-	B@AP

Internal VLAN ID:
 Multicast Support:

Figure 34: Network Topologies

- 3 To change any of the associated Admin parameters, click on the Admin topology entry. The **Edit Topology** dialog appears.

Figure 35: Edit Topology

- 4 Under Core, the Admin port **Name** and **Mode** are not configurable.
- 5 Under Layer 3 - IPv4, the following settings are available:

The **Static IP Address** specifies the address assigned by the administrator.

In the **Mask** field, type the appropriate subnet mask for the IP address (typically, 255.255.255.0).

The **MTU** value specifies the Maximum Transmission Unit or maximum packet size for this topology. The fixed value is 1500 bytes for physical topologies. 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 52).

The **Gateway** field specifies the IP address of the default gateway for the Admin port.

- 6 Under Layer 3 - IPv6, the following settings are available:
 - The **Static IPv6 Address** field specifies the address assigned by the administrator.
 - The **Static IPv6 Gateway** field specifies the IP address of the default gateway for the Admin port.
 - The **Prefix Length** field specifies the length of the IPv6 prefix. Maximum is 64 bits.
 - The **MTU** value specifies the Maximum Transmission Unit or maximum packet size for this topology. The fixed value is 1500 bytes for physical topologies. 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 52).
 - The **Dynamic IP Address** lists the current auto-generated IPv6 addresses assigned to the Admin port.

Note

IPv6 supports multiple addresses on the same port including auto-generated addresses such as a link-local address, or an address created by combining the Router Advertisement prefix with the interface ID. Auto-generated addresses generated via the Router Advertisement prefix are dynamic and their availability depends on the existence of the prefix (or lack of) in the Router Advertisement.

- 7 Click **Refresh** to refresh the list of Dynamic IP Addresses and click **Save** .
Or, click **Cancel** to close the Edit Topology dialog without saving any changes to the port configuration.

Configuring a Basic Data Port Topology

To configure a basic data port topology:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **Topologies**. The **Topologies** window displays.

The screenshot shows the VNS interface with the 'Topologies' window open. The left sidebar shows a tree view with 'Topologies' selected. The main window displays a table of topologies:

Topology Name	Group	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	✗	-	✗	Admin	Static: 192.168.3.71 Dynamic IP Address	Admin
<input type="checkbox"/> Bridged at AP untagged	✗	4093	✗	-	-	B@AP
<input type="checkbox"/> g1	✓	22	✗	-	-	B@EWC
<input type="checkbox"/> physical 1	✗	111	✗	esa0	10.71.0.1	Physical
<input type="checkbox"/> t1	✗	2	✓	esa0	-	B@EWC
<input type="checkbox"/> t2	✗	3	✓	esa0	-	B@EWC

Below the table are buttons: **New**, **New Group**, and **Delete Selected**. There are also input fields for **Internal VLAN ID:** 1 and **Multicast Support:** Disabled. A **Save** button is at the bottom right.

Figure 36: Configuring a Topology

- 2 Select the topology to edit or click **New** to create a new topology.
For more information, see [Configuring a Basic Topology](#) on page 224.

Configuring a Basic Topology

To configure a basic topology:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **Topologies**. The **Topologies** window displays.

- 2 Select the topology to edit or click **New** to create a new topology.

Figure 37: Configuring a basic topology

- 3 On the **General** tab, enter a name for the topology in the **Name** field.
- 4 Select a mode of operation from the **Mode** drop-down list. Choices are:
 - **Physical** — VLAN identifier (1 - 4094), with at least one layer 2 member port (no mu associated).
 - **Routed** — Routed topologies do not require Layer 2 configuration (controller internal VLAN identifier from valid range 1- 4094), and Layer 3 configuration. See [Layer 3 Configuration](#) on page 228 for more information.
 - **Bridge Traffic Locally at AP** — Requires Layer 2 configuration. Does not require Layer 3 configuration. Bridge Traffic at the AP VNSs do not require the definition of a corresponding IP address since all traffic for users in that VNS will be directly bridged by the Wireless AP at the local network point of attachment (VLAN at AP port).
 - **Bridge Traffic Locally at EWC** — Requires Layer 2 configuration. May optionally have Layer 3 configuration. Layer 3 configuration would be necessary if services (such as , captive portal, etc.) are required over the configured network segment, or if controller management operations are intended to be done through the configured interface.

- 5 Configure the Layer 2 **VLAN Settings**, depending on the previously selected Mode.
 - For **Physical**, enter a VLAN identifier (2 - 4094), with at least one layer 2 member port (no mu associated).
 - For **Bridge Traffic Locally at EWC**, enter a VLAN identifier (2- 4094) that is valid for your system and enter the port to which this VLAN is attached to, according to the networking deployment model pre-established during planning.
 - For **Bridge Traffic Locally at AP**, enter a VLAN identifier (1 - 4094), 4094 is reserved for Internal VLAN ID.
 - Specify whether the VLAN configuration is **Tagged** or **Untagged**.
 - To eliminate ARP Request Broadcast on the Wireless network, select **ARP Proxy**. ARP Proxy applies to traffic for **Bridge Traffic Locally at AP** Topologies. ARP Proxy is configurable per topology.
 - For **Port**, select the Physical (Ethernet) or data port. For more information, see [Viewing and Changing the L2 Ports Information](#) on page 53.
- 6 Click **Save** to save your changes.

These steps are sufficient to create and save a topology. The following configuration options are optional and depend on the mode of the topology.

Creating a Topology Group

A topology group is a list of topologies with a unique name and a VLAN ID of its own. A topology group's name must be unique across topology groups and topologies since it will be used anywhere the topology name can be used. All the topologies in a defined group have the same type. For example, if the topology group mode is Routed, it only contains Routed topologies. The maximum number of topology groups for all platforms is 32.

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Topologies**.

- 3 On the **Topologies** tab, click **New Group**.

Topology Group:

General

Core

Name:

Mode: Routed ▼

Layer 2

VLAN Setting: VLAN ID: (1 - 4094)

Topologies

Topology Name ↕	VLAN ID ↕	Tagged ↕	Port ↕	IP Address ↕

Figure 38: Topology Group

- 4 Under **Core**, enter a name for the topology group.
- 5 Under **Mode**, select a mode from the drop-down menu. Choices are Bridge Traffic Locally at EWC and Routed.
- 6 Under **Layer 2, VLAN Setting**, enter a VLAN ID (1-4094).
- 7 Under **Topologies**, only the topologies of the group's type are shown & eligible for inclusion. Select topologies to be members of the group. A topology group must contain at least 1 topology.
- 8 Click **Save**.

Edit or Delete a Topology Group

To modify or delete a topology group:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Topologies** and click on a topology group to edit or delete. (Do not select the checkbox.)
- 3 To edit the group, in the Topologies pane, click **Edit**.
The Topology list is populated with available topologies.
- 4 Check topology boxes to add topologies to the group. Clear the checkboxes to remove topologies from the group.
- 5 To delete the topology group that you have open, click the **Delete** button.
When a topology group is deleted, only the group is deleted, not the topologies it contains.
- 6 Click **Save**.

- 7 You can also delete the topology group from the **Topologies** tab.
 - a From the top menu, click **VNS**.
 - b From the left pane, click **Topologies**.
 - c Select the checkbox for the topology group to delete and click **Delete Selected**.
 - d Click **Save**.

Enabling Management Traffic

If management traffic is enabled for a VNS, it overrides the built-in exception filters that prohibit traffic on the controller data interfaces. For more information, see [Policy Rules](#) on page 243.

To enable management traffic for a topology:

- 1 From the top menu, click either **Controller** or **VNS**. Then, in the left pane, select **Topologies**.
- 2 Select the desired physical or Routed topology. If the Layer 3 parameters are not displayed, check the **Layer 3** checkbox.
- 3 Select the **Management Traffic** checkbox.
- 4 Click **Save**.

Layer 3 Configuration

This section describes configuring IP addresses, options, Next Hop and OSPF parameters, for Physical port, Routed, and Bridge Traffic Locally at EWC topologies.



Note

IPv6 is not supported in Layer 3 configuration.

IP Address Configuration


The L3 (IP) address definition is only required for Physical port and Routed topologies. For Bridge Traffic Locally at EWC topologies, L3 configuration is optional. L3 configuration would be necessary if services such as , captive portal, AP registration (with up to 4 topologies) are required over the configured network segment or if controller management operations are intended to be done through the configured interface.

Bridge Traffic Locally at AP VNSs can be a defined Mask and do not require the definition of a corresponding IP address since all traffic for users in that VNS will be directly bridged by the AP at the local network point of attachment (VLAN at AP port).

To define the IP address for the topology:

- 1 From the top menu, click **Controller > Topologies**, or **VNS > Topologies**.
- 2 Click **New** to create a new topology or select the topology you want to define the IP address for. The **Topologies** window is displayed. Depending on the preselected options, two or three tabs are displayed.

Figure 39: Configuring IP Address for Routed Topology

- 3 For IP interface configuration for **Routed** topologies, configure the following Layer 3 parameters.
 - a In the **Gateway** field, type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to MUs (in the VNS) as the default gateway for the VNS subnet. (MUs target the controller's interface in their effort to route packets to an external host).
-
- 

Note
The Gateway field only supports IPv4 addresses.
-
- b In the **Mask** field, type the appropriate subnet mask for the IP address. to separate the network portion from the host portion of the address (typically, 255.255.255.0).
 - c If desired, enable Management traffic.
 - 4 For IP interface configuration for **Bridge Traffic Locally at EWC Topologies**, configure the following Layer 3 parameters.

- 1 In the **Interface IP** field, type the IP address that corresponds to the controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.
- 2 In the **Mask** field, type the appropriate subnet mask for the IP address. to separate the network portion from the host portion of the address (typically, 255.255.255.0).
- 3 Configure Strict Subnet Adherence.
- 4 If desired, configure AP Registration. If selected, wireless APs can use this port for discovery and registration.
- 5 If desired, enable Management traffic.

Figure 40: IP Address for Bridged Traffic Locally

DHCP Configuration

You can configure settings for all modes except **Bridge Traffic Locally at AP** mode since all traffic for users in that VNS will be directly bridged by the AP at the local network point of attachment (VLAN at AP port). DHCP assignment is disabled by default for Bridged to VLAN mode. However, you can enable DHCP server/relay functionality to have the controller service the IP addresses for the VLAN (and wireless users).

To configure DHCP options:

- 1 Click **VNS > Topologies > General** and enable Layer 3.
- 2 From the **DHCP** drop-down list, select one of the following options and click **Configure**.
 - **Local Server** if the controller's local DHCP server is used for managing IP address allocation.

- **Use Relay** if the controller forwards DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.
- 3 If you selected **Local Server**, the following window displays. Configure the following parameters:

- 1 In the **Domain Name** box, type the external enterprise domain name server to be used.
- 2 In the **Lease default** box, type the default time limit. The default time limit dictates how long a wireless device can keep the DHCP server assigned IP address. The default value is 36000 seconds (10 hours).
- 3 In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
- 4 In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
- 5 Check the **Enable DLS DHCP Option** checkbox if you expect optiPoint WL2 wireless phone traffic on the VNS. DLS is a Siemens application that provides configuration management and software deployment and licensing for optiPoint WL2 phones.
- 6 In the **Gateway** field, type the controller's own IP address in that topology. This IP address is the default gateway for the topology. The controller advertises this address to the wireless devices when they sign on. For routed topologies, it corresponds to the IP address that is communicated to wireless clients as the default gateway for the subnet. (wireless clients target the controller's interface in their effort to route packets to an external host).

For a Bridge traffic locally at the EWC topology, the IP address corresponds to the controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.

- 7 The **Address Range** boxes (from and to) populate automatically with the range of IP addresses to be assigned to wireless devices using this VNS, based on the IP address you provided.
 - To modify the address in the **Address Range from** box, type the first available address.
 - To modify the address in the **Address Range to** box, type the last available address.
 - If there are specific IP addresses to be excluded from this range, click Exclusion(s). The **DHCP Address Exclusion** dialog is displayed.

Figure 42: DHCP Address Exclusion

- In the **DHCP Address Exclusion** dialog, do one of the following:
 - To specify an IP range, type the first available address in the **From** box and type the last available address in the **to** box. Click **Add** for each IP range you provide.
 - To specify an IP address, select the **Single Address** option and type the IP address in the box. Click **Add** for each IP address you provide.
 - To save your changes, click **OK**.
- 1 The **Broadcast Address** box populates automatically based on the Gateway IP address and subnet mask of the VNS.
 - 2 Click **Close**.

Figure 41: DHCP Configuration

- 4 If you selected **Use Relay**, a **DHCP** window displays.
 - a in the **DHCP Servers** box, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

Note



The DHCP Server must be configured to match the topology settings. In particular for Routed topologies, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.

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

Defining a Next Hop Route and OSPF Advertisement

The next hop definition allows the administrator to define a specific host as the target for all non-VNS targeted traffic for users in a VNS. The next hop IP identifies the target device to which all VNS (user traffic) will be forwarded to. Next-hop definition supersedes any other possible definition in the routing table.

If the traffic destination from a wireless device on a VNS is outside of the VNS, it is forwarded to the next hop IP address, where this router applies role and forwards the traffic. This feature applies to unicast traffic only. In addition, you can also modify the Open Shortest Path First (OSPF) route cost.

OSPF is an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately distributes the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place.

To define a Next Hop Route and OSPF Advertisement:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **Topologies** pane, then click the Routed topology for which you want to define a next-hop route.
- 3 In the Layer 3 area, click the **Configure** button. The configuration dialog displays.

Figure 43: DHCP configuration

- 4 In the **Next Hop Address** box, type the IP address of the next hop router on the network through which you wish all traffic on the VNS using this Topology to be directed.

- 5 In the **OSPF Route Cost** box, type the OSPF cost of reaching the VNS subnet.
The OSPF cost value provides a relative cost indication to allow upstream routers to calculate whether or not to use the controller as a better fit or lowest cost path to reach devices in a particular network. The higher the cost, the less likely of the possibility that the controller will be chosen as a route for traffic, unless that controller is the only possible route for that traffic.
- 6 To disable **OSPF advertisement** on this VNS, select the **Disable OSPF Advertisement** checkbox.
- 7 Click **Close**.
- 8 Click **Save**.

Exception Filtering

The exception filter provides a set of rules aimed at restricting the type of traffic that is delivered to the controller. By default, your system is shipped with a set of restrictive filter rules that help control access through the interfaces to only those services that are absolutely necessary.

By configuring to allow management on an interface, an additional set of rules is added to the shipped filter rules that provide access to the system's management configuration framework (SSH, HTTPS, SNMP Agent). Most of this functionality is handled directly behind the scenes by the system, rolling and unrolling canned filters as the system's topology and defined access privileges for an interface change.



Note

An interface for which Allow Management is enabled can be reached by any other interface. By default, Allow Management is disabled and shipped interface filters will only permit the interface to be visible directly from its own subnet.

The visible exception filter definitions, both in physical ports and topology definitions, allow administrators to define a set of rules to be added to the system's dynamically updated exception filter protection rules. Rule evaluation is performed top to bottom, until an exact match is determined. Therefore, these user-defined rules are evaluated before the system's own generated rules. As such, these user-defined rules may inadvertently create security lapses in the system's protection mechanism or create a scenario that filters out packets that are required by the system.



Note

Use exception filters only if absolutely necessary. It is recommended that you avoid defining general allow all or deny all rule definitions since those definitions can easily be too liberal or too restrictive to all types of traffic.

The exception rules are evaluated in the context of referring to the specific controller's interface. The destination address for the role rule definition is typically defined as the interface's own IP address. The port number for the filter definition corresponds to the target (destination) port number for the applicable service running on the controller's management plane.

The exception filter on an topology applies only to the packets directed to the controller and can be applied to the destination portion of the packet, or to the source portion of the packet when filtering is enabled. Traffic to a specified IP address and IP port is either allowed or denied. Adding exception filter rules allows network administrators to either tighten or relax the built-in filtering that automatically drops packets not specifically allowed by role rule definitions. The exception filter rules can deny access in the event of a DoS attack, or can allow certain types of management traffic that would otherwise be denied. Typically, Allow Management is enabled.

To define exception filters:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, select **Topologies**.
- 3 On the **Topologies** page, click the **Exception Filters** tab.

The **Exceptions Filter** page displays.

The screenshot shows the NCM interface for configuring exception filters. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar shows a tree view with 'Topologies' selected. The main content area is titled 'Topology: CNL-422-2-11' and has three tabs: 'General', 'Multicast Filters', and 'Exception Filters'. The 'Exception Filters' tab is active, displaying a table of filters:

Rule	In	Allow	IP : Port	Protocol
I	dest	<input type="checkbox"/>	10.219.46.89/32:60606	TCP
I	dest	<input type="checkbox"/>	0.0.0.0/32:50200	TCP
I	dest	<input checked="" type="checkbox"/>	10.219.46.89/32:32768-65535	TCP
I	dest	<input checked="" type="checkbox"/>	10.219.46.89/32:32768-65535	UDP
I	dest	<input checked="" type="checkbox"/>	10.219.46.89/32:67 (DHCP Server)	UDP
I	dest	<input checked="" type="checkbox"/>	255.255.255.255/32:67 (DHCP Server)	UDP
I	dest	<input checked="" type="checkbox"/>	10.219.46.89/32	ICMP
I	dest	<input checked="" type="checkbox"/>	10.219.46.89/32:80 (HTTP)	TCP
I	dest	<input checked="" type="checkbox"/>	10.219.46.89/32:443 (HTTPS)	TCP
I	dest	<input checked="" type="checkbox"/>	10.219.46.89/32:443	UDP

Below the table are buttons for 'Up', 'Down', 'Add', 'Delete', and 'Add Predefined'. A 'Select filter' dialog box is open, showing fields for 'IP/subnet:port' (0.0.0.0/0), 'Protocol' (N/A), and 'In Filter' (Destination(dest)).

Figure 44: Topology Exception Filters

- 4 Select an existing topology from the right-hand pane to edit an existing topology, or click **New** to create a new topology.

The **Topologies** configuration page displays. The Exception Filters tab is available only if Layer 3 (L3) configuration is enabled.

- 5 Click the **Exception Filters** tab to display the **Exception Filters** page.

Table 33: Exception Filters page - Fields and Buttons

Field/Button	Description
Rule	Identifies the type of role rule. Options are: <ul style="list-style-type: none"> • D - Default rule • I - Internal (read-only) • T - Local interface rule • U - user-defined rule
In	Identifies the rule that applies to traffic from the network host or wireless device that is trying to get to a controller. You can change this setting using the drop-down menu. Options include: <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only
Allow	Select the Allow checkbox to allow this rule. Otherwise the rule is denied.
IP:Port	Identifies the IP address and port to which this role rule applies.
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
Up, Down	Select a role rule and click to either move the rule up or down in the list. The filter rules are executed in the order in which you define them here
Add	Click to add a role rule. The fields in the Add Filter area are enabled.
Delete	Click to remove this role rule.
Add Predefined	Select a predefined role rule. Click Add to add the rule to the rule table, otherwise click Cancel
Save	Click to save the configuration.
Advanced Mode	Advanced filtering mode provides the ability to create bidirectional filters. If this controller participates in a mobility zone, before enabling advanced mode be sure that all controllers in the mobility zone are running V7.41 or greater. Note: After enabling advanced filtering mode, you can no longer use NMS Wireless Manager V4.0 to manage the controller's roles and you cannot switch back to basic filter mode unless you return the controller to its default state.
Add Filter section	
IP/subnet:port	Type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.

Table 33: Exception Filters page - Fields and Buttons (continued)

Field/Button	Description
In Filter	<p>In the drop-down menu, select an option that refers to traffic from the network host that is trying to get to a wireless device. Options include:</p> <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>By default, user-defined rules are enabled on ingress (In), and are assumed to be Allow rules. To disable the rule in either direction, or to make it a Deny rule, click the new filter, then de-select the relevant checkbox.</p>
OK	Click to add the role rule to the filter group. The information displays in the role rule table.
Cancel	Click Cancel to discard your changes.

**Note**

For External Captive Portal, you need to add an external server to a non-authentication filter.

Multicast Filtering

A mechanism that supports multicast traffic can be enabled as part of a topology definition. This mechanism is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control.

**Note**

To use the mobility feature with this topology, you must select the **Enable Multicast Support** checkbox for the data port.

Define a list of multicast groups whose traffic is allowed to be forwarded to and from the VNS using this topology. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.

**Note**

Before enabling multicast filters and depending on the topology, you may need to define which physical interface to use for multicast relay. Define the multicast port on the **IP Addresses** tab. For more information, see [Setting Up the Data Ports](#) on page 52.

To enable Multicast for a topology:

- 1 On the **Topologies** page, click the **Multicast Filters** tab.

Logs Reports Controller AP **VNS** Radar

Topology: AH-BAC-2005

General
Multicast Filters

Multicast bridging (only the multicasts matching the rules defined will be allowed)

IP	Group	Wireless Replication i
ff00::/8	All V6 Multicast	<input checked="" type="checkbox"/>
ff02::fb/128	mDNSV6/Bonjour	<input checked="" type="checkbox"/>
ff05:2005::16/32		<input checked="" type="checkbox"/>

IP Group:

Defined groups:

Figure 45: Topology Multicast Filters

- 2 To enable the multicast function, select **Multicast bridging**.
- 3 Define the multicast groups by selecting one of the radio buttons:
 - **IP Group** – Type the IP address range.
 - **Defined groups** – Click from the drop-down list.



Note

IPv6 traffic is supported for B@AC and B@AP topologies.

- 4 To enable the wireless multicast replication for this group, select the corresponding **Wireless Replication** checkbox. Wireless Replication filters multicast traffic being sent back to the wireless AP channel or wired network.

**Note**

Wireless replication takes effect only when Multicast Address is allowed.

- 5 Click **Add**. The group is added to the list above.
- 6 To modify the priority of the multicast groups, click the group row, and then click the **Up** or **Down** buttons.

A Deny All rule is automatically added as the last rule, IP = *.*.* and the **Wireless Replication** checkbox is not selected. This rule ensures that all other traffic is dropped.

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

**Note**

The multicast packet size should not exceed 1450 bytes.

6 Configuring Roles

Roles Overview

Configuring Default VLAN and Class of Service for a Role Policy Rules

Roles Overview

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

A role can contain any number of services in Policy Manager.

A VNS can have up to two roles assigned to it. The default non-authenticated role will be used while the station is not authenticated but able to access the network. The default authenticated role will be assigned to a station if it completes authentication successfully but the authentication process did not explicitly assign a role to the station.

A role may also contain default access control (VLAN) and/or Class of Service (priority) characteristics that will be applied to traffic not identified specifically by the set of access services contained in the role. The set of services included in a role, along with any access control or class of service defaults, determine how all network traffic will be handled at any network point configured to use that role.

Roles don't need to be fully specified; unspecified attributes are retained by the user or inherited from Global Role definitions (see [Configuring the Global Default Policy](#) on page 360 for more information).

Default Global Role definitions provide a placeholder for completion of incomplete roles for initial default assignment. If a role is defined as Default for a particular VNS, the role inherits incomplete attributes from Default Global Role definitions.

Configuring Default VLAN and Class of Service for a Role

From the **VLAN & Class of Service** tab you can assign a previously configured topology to a role. You can also launch the Topology Configuration page to edit an existing topology or create a new one. For information about how to configure a topology, refer to [Configuring a Basic Data Port Topology](#) on page 223.

Note



The Configuration Manager (CM) checks overall configuration as configuration is entered. If CM detects mixed B@AC and B@AP rules in the same role, and the role has L7 filter rules, then the configuration is rejected. For more information, see [Configuration Rules with L7 Filters](#) on page 262.

In general, 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 the role is permitted. The CoS defines actions to be taken when rate limits are exceeded.

To configure VLAN and Class of Service for a role:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **Roles** pane and click the role you want to edit, or click **New** to create a new role.

The screenshot shows the configuration page for a role named 'r1' under the 'VNS' menu. The 'VLAN & Class of Service' tab is active, showing the following configuration:

- Core:** Role Name: r1
- Default Action:**
 - Access Control: Allow
 - Default Class of Service: No change
 - Traffic Mirror: None
- HTTP Redirection:**
 - Redirection URL: (Lab126-12-Ext-CP) http://192.168.11.22:/login:

Note: token=<integer_val>&dest=<original_target_url>&hwcip=<hwc_ip>&hwcpport=<hwc_port> will be APPENDED to the redirection URL

Buttons: New, Delete, Save, Advanced...

Figure 46: VLAN & Class of Service Tab

- 3 Select **Policy Rules** to configure the policy rules for the Role. For more information, see [Configuring Policy Rules](#) on page 254.

Table 34: VLAN & Class of Service Tab - Fields and Buttons

Field/Button	Description
Core	
Role Name	Enter a name to assign to this role.
Default Action	
Access Control	<p>Select from one of the following:</p> <ul style="list-style-type: none"> • 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.
VLAN	<p>Note: VLAN is only visible when the user selects "Contain to VLAN" as the default access control action.</p> <p>Select an existing Topology, Topology Group, or click New to create a new Topology. To edit an existing Topology, select the VLAN and then click Edit. The Edit Topology page displays. For more information, see Configuring a Basic Topology on page 224.</p>
Default Class of Service	<p>Select an existing class of service from the Default Class of Service drop-down list, or click New to create a new topology. To edit an existing class of service, select the class of service and then click Edit. The Edit Class of Service page displays. For information about how to configure a Class of Service, go to Classes of Service Overview on page 439.</p>
Traffic Mirror	<p>When enabled, this option sends a copy of the network packets to a mirroring L2 port for analysis, in an effort to monitor network traffic. The Purview Engine analyses the traffic, and the assigned port can only be used for traffic analysis.</p> <p>You can enable traffic mirroring from the WLAN Service, from the Role, or from the Filter Rule. Setting traffic mirroring at the Filter Rule takes precedence over settings for the Role and WLAN Service. The order of precedence for the traffic mirror setting is: Filter Rule, Role, WLAN Service. To set the port number, go to VNS > Global > Netflow/MirrorN Configuration.</p> <p>Valid values for Filter Rule and Role are:</p> <ul style="list-style-type: none"> • None - No traffic mirroring • Enable - Traffic mirroring enabled. Traffic is copied if the filter rule matches or the role is applied. • Prohibited - Traffic mirroring is prohibited for this role. Traffic is not copied when the filter rule matches or the role is applied. <p>Valid values for the WLAN Service are:</p> <ul style="list-style-type: none"> • Prohibited - Traffic is not copied for this WLAN Service. • Enable in both directions - Traffic coming from wireless clients and traffic targeted at specific clients is copied. • Enable in direction only - Traffic generated by wireless clients only is copied.

Table 34: VLAN & Class of Service Tab - Fields and Buttons (continued)

Field/Button	Description
HTTP Redirection	<p>HTTP Redirection appears when the following conditions are present:</p> <ul style="list-style-type: none"> • Rule-based Redirection is enabled on the Filtering Mode screen. • A filter exits with Access Control = HTTP Redirect. <p>(See Understanding the Filter Rule Definition Dialog on page 257.)</p>
Redirection URL:	<p>Select from one of the previously configured redirection URLs or click New to create a new redirection URL. For more information about setting up a redirection URL, see Managing Redirection URLs on page 372. WLANs with Captive Portals are included in this list.</p> <p>The default value for the redirection URL is Own WLAN, which indicates the current WLAN. This is identical to the current redirection behaviour.</p>
Status	
Synchronize	<p>Enable automatic synchronization with its availability peer. For more information about viewing synchronization status, see Using the Sync Summary on page 365. If this VNS is part of an availability pair, Extreme Networks recommends that you enable Synchronize. By default the WLAN Service is enabled. Clear this checkbox to disable the WLAN Service.</p>
Advanced Button	
Static Egress Untagged VLANs	<p>Lists those VLANs (for multicast, broadcast, unicast) that a station assigned to a role receives from, even if it hasn't sent on it. Choose a VLAN as follows:</p> <ul style="list-style-type: none"> • Click a VLAN from the list of available VLANs to use • Click >> to move the VLAN to the active list of VLANs used • Click OK to permit static configuration of egress untagged VLANs.

For more information about rate control profiles, see [Working with Bandwidth Control Profiles](#) on page 359.

Policy Rules

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

ExtremeWireless supports IPv6 prefixes specified in policy filter rules. With a few considerations:

- 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 .
- Application visibility rules are ignored for http[s] flows over IPv6.

Related Links

[Understanding the Filter Rule Definition Dialog](#) on page 257

[L7 Configuration](#) on page 262

Matching Policy Rules Criteria

The following criteria apply when trying to match rules. Many of these criteria accept a range of addresses or codes not just a single address or code.

A policy rule consists of:

- Match criteria
- An optional access control action (allow, deny)
- An optional class of service assignment

Policy rules can match on:

- Source MAC address
- Destination MAC address
- IPv4 or IPv6 Source IP address
- IPv4 or IPv6 Destination IP address
- Source layer 4 port
- Destination layer 4 port
- IPv4 or IPv6 Source socket (IP address + port)
- IPv4 or IPv6 Destination socket (IP address + port)
- IP type
- packet type and code
- ToS/DSCP marking
- 802.1p priority
- Ethertype

Policy rule access control actions can be:

- Allow — Forward matching frames on the WLAN Service's default topology.
- Deny — Drop matching frames.
- Contain to VLAN — Forward matching frames on the indicated VLAN.
- None — The rule does not have an access control action. The matching engines ignore a rule with an access control action of 'None'.
- HTTP Redirect — Redirect traffic to default URL 'Own WLAN' or to a URL that is defined on the **Redirection URL** screen. For more information, see [Managing Redirection URLs](#) on page 372. You can also specify a Redirection URL when you configure an External Captive Portal. For more information, see [Configuring Firewall Friendly External Captive Portal](#) on page 306.

Rule-Based Redirection

You can now configure policy rules to explicitly redirect traffic to the captive portal definition assigned to the role, regardless of authentication status. Rule-based Redirection applies to HTTP and HTTPS traffic, and explicitly defines when traffic will be redirected. In previous releases, redirection automatically redirected an un-authenticated client to an ECP when a deny action on HTTP(S) traffic occurred.

Rule-based redirection requires explicit enablement. For new installations, Rule-based Redirection is enabled by default. For upgrades from releases prior to v10.11, ExtremeWireless preserves the previous captive portal redirection method of triggering redirect off denied HTTP/HTTPS for non-authenticated roles.

To enable Rule-based Redirection upon an upgrade, go to **VNS > Global > Filtering Mode**.

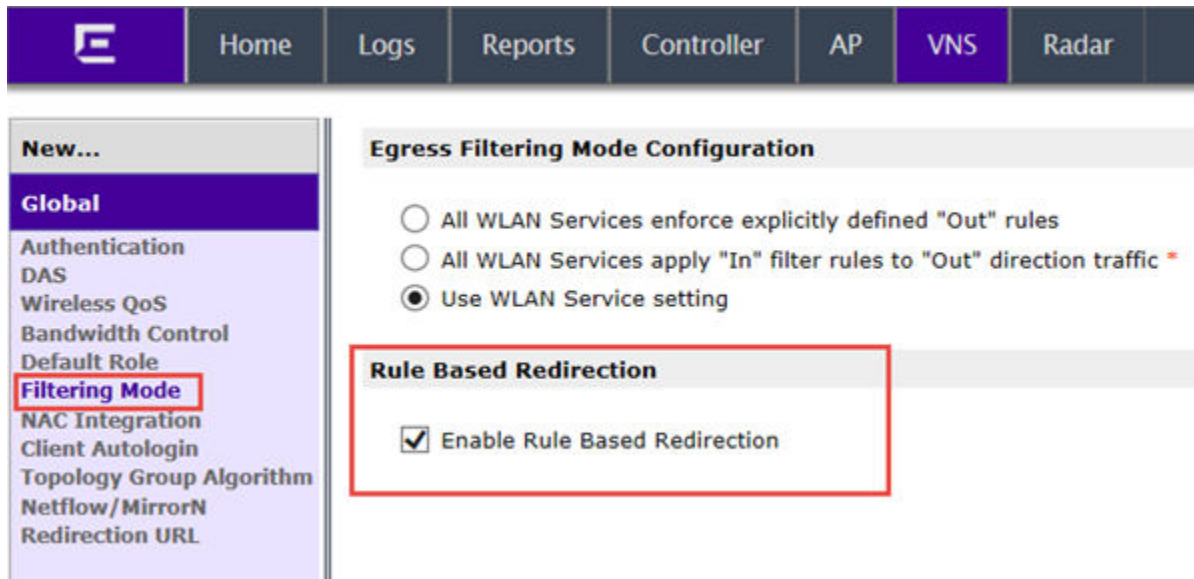


Figure 47: Enabling Rule-based Redirection

To use Rule-based Redirection:

- Verify that the feature is enabled.
- Configure roles with policy rules for redirection. Add the Redirect rules to the (non-auth) role definition; otherwise, the Deny All default action is interpreted explicitly, and traffic will be denied not redirected.
- Configure a list of redirection URLs.
- Specify the redirection URL on the Role **VLAN & Class of Service** tab. This value can be an IP address, URL, or host name if using L7 host name rules.
- (Optional) If you are redirecting to a captive portal, configure the captive portal for redirected traffic.

Rule-based Redirection is explicit when the redirection flag is enabled and a rule is defined for redirection. The redirection destination can be defined on the role or as part of a WLAN Service configuration. If a redirection destination is not configured, the default destination is 'Own WLAN', which indicates the WLAN of the device. Redirection is allowed on any port.

Figure 48: Example Role with Redirection to ECP specified.

Related Links

[Understanding the Filter Rule Definition Dialog](#) on page 257

[Host Name DNS Support](#) on page 267

[Managing Redirection URLs](#) on page 372

[Configuring Firewall Friendly External Captive Portal](#) on page 306

[Configuring External and Mode 802.1 Captive Portal](#) on page 304

[Configuring Default VLAN and Class of Service for a Role](#) on page 240

Configuring Rule-Based Redirection

Deciding how to configure HTTP Redirection depends on the type of traffic you are allowing and the default Access Control value you configure on the role. You must configure the policy rules in the following order:

- Allow policies
- Redirect policies (if using Rule-based Redirection)
- Deny policies.

Allow Policies

You can configure five Allow policies or any combination of Allow and Deny policies on a single role. The following are ways to implement policy rules:

- Allow All Policy.

If you opt to allow all traffic. You only need one policy rule indicating that all traffic is allowed.

Layer 2,3,4 Classification

Layer 2

Ethertype: Internet Protocol, Version 4 (IPv4) 0x0800

Mac Address: Any Mac 00:00:00:00:00:00/0

Priority: Any Priority

Layer 3,4

IP/subnet: Any IP Address 0.0.0.0/0

Port: Any Port 0

Protocol: Any Protocol 0

ToS/DSCP: 0x (DSCP:) Select Mask: 0xFF

Application

Application: none

Action

Access Control: Allow

Class of Service: None

Traffic Mirror: None

Figure 49: Allow All Policy Configuration

- Combination of Allow and Deny policies, allowing specific traffic.

Role: bapUnauth

VLAN & Class of Service | Policy Rules

Inherit filter rules from currently applied role

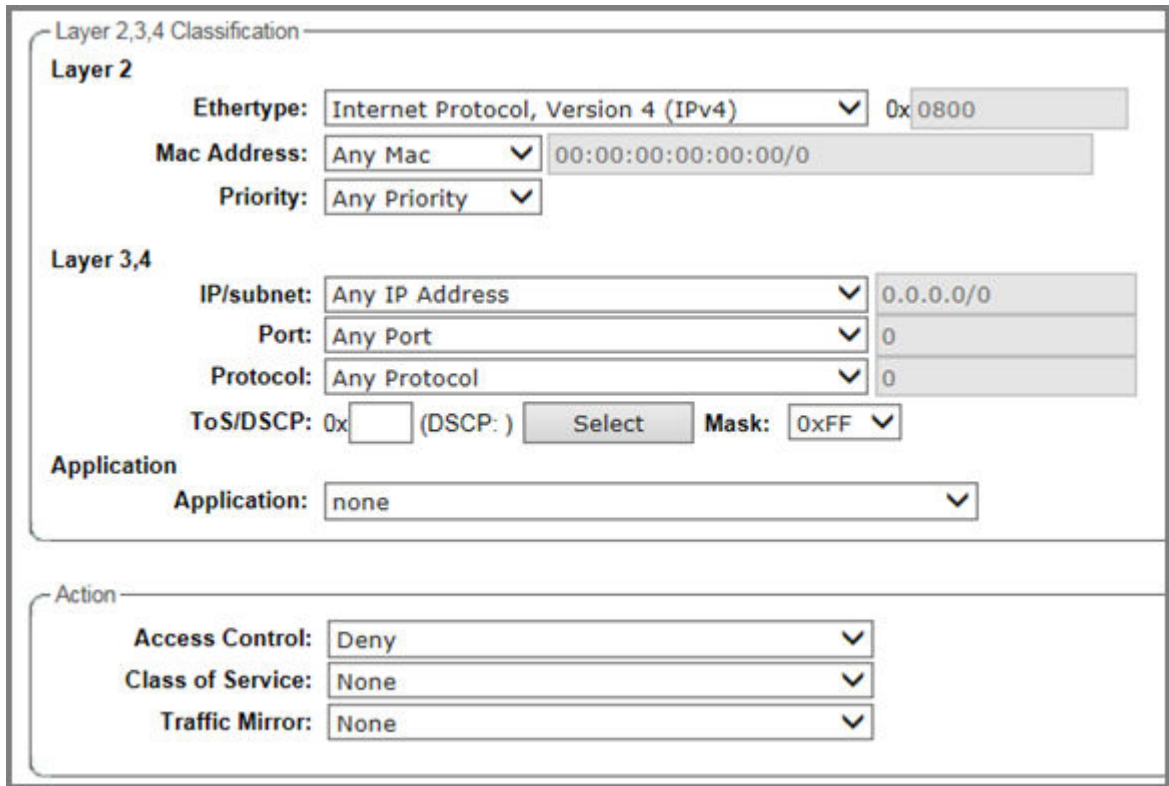
Rules AP Filtering Custom AP Rules

Action	Name	Protocol	QoS	In	Out
Allow	0.0.0.0/0:68 (DHCP Client)	UDP	None	both	both
Allow	0.0.0.0/0:67 (DHCP Server)	UDP	None	both	both
Allow	192.0.1.203/32	Any	None	both	both
Deny	0.0.0.0/0	Any	None	both	both

Figure 50: Policy Rules Configuration

- Deny All Policy.

When opting to deny all traffic, you must first configure the 5 Allow policies to gather the parameters that direct the client to the FFECF. First configure the specific Allow policies, then configure the Deny All policy.



Layer 2,3,4 Classification

Layer 2

Ethertype: Internet Protocol, Version 4 (IPv4) 0x0800

Mac Address: Any Mac 00:00:00:00:00:00

Priority: Any Priority

Layer 3,4

IP/subnet: Any IP Address 0.0.0.0/0

Port: Any Port 0

Protocol: Any Protocol 0

ToS/DSCP: 0x (DSCP:) Select Mask: 0xFF

Application

Application: none

Action

Access Control: Deny

Class of Service: None

Traffic Mirror: None

Figure 51: Deny All Policy Configuration

- Redirect Policy
 - If Rule-based Redirection is enabled, configure at least one policy rule where the Access Control is set to **HTTP Redirect**.
 - If Rule-based Redirection is disabled, configure at least one policy rule where the Access Control is set to **Deny**.



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 .

For more information on configuring policy rules, see [Understanding the Filter Rule Definition Dialog](#) on page 257 in the *User Guide*.

Related Links

[Configuring Rule-Based Redirection](#) on page 246

[Understanding the Filter Rule Definition Dialog](#) on page 257

[Rule-Based Redirection](#) on page 244

[Host Name DNS Support](#) on page 267

[Configuring a Captive Portal on an AP](#) on page 196

Rule Based Redirection to a Captive Portal

Redirecting to a captive portal is a common rule-based redirection use case. The following is an example Allow configuration for rule-based redirection to a captive portal.

- The role allows the station to use DHCP and DNS:
 - Access Control = **Allow**, Port = **DNS**
 - Access Control = **Allow**, Port = **DHCP Client**.
 - Access Control = **Allow**, Port = **DHCP Server**.
- The role allows the station to communicate with the external captive portal server using HTTP or HTTPS.
 - Access Control = **Allow**, IP/subnet = IP of Captive Portal Server

Then specify the Captive Portal Server on the **VLAN Class of Service** tab in the **Redirection URL** field. The Redirection URL can be provided as a URL, IP address, or host name if using L7 Host Name DNS support.

- The role must allow the station to send traffic to the controller's IP address on the VLAN containing the station's traffic; therefore, one Allow policy must include the IP/subnet that corresponds to the VLAN ID. Depending on the Default Access Control value on the role, this can be the VLAN ID specified on the role or the VLAN ID specified during WLAN Service configuration.
 - When default Access Control = Allow, VLAN ID on the WLAN Service configuration is used.
 - When default Access Control = Contain to VLAN, the VLAN ID on the Role configuration is used.
- Access Control = **Allow**, IP/subnet = Configured VLAN subnet.



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 .

Policy Rules for a Non-authenticated Role

A VNS' non-authenticated role controls the access of stations until the station completes authentication. The role can be as restrictive or open as necessary. If the station is expected to authenticate, then the role may need to grant it access to resources required to complete the authentication. For example if the station is expected to perform captive portal authentication then the non-authenticated role must allow the station to:

- Perform address acquisition
- DNS name lookups
- ARP lookups
- Forward to the Captive Portal web server

The administrator may grant unauthenticated stations access to other resources, but the recommended default action of a non-authenticated role is to drop all traffic that does not match a rule.

Defining non-authenticated roles allows administrators to identify destinations that a mobile user is allowed to access without incurring an authentication redirection. Typically, the recommended default rule is Deny All. However, administrators should define a rule set that permits users to access essential services:

- DNS (IP of DNS server)

- Default Gateway (VNS Interface IP)

Any HTTP streams requested by the client for denied targets is redirected to the specified location.

The non-authenticated role should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. This filter should also allow network access to the IP address of the DNS server and to the network address—the gateway of the Topology. The gateway is used as the IP for an internal Captive Portal page. An external Captive Portal provides a specific IP definition of a server outside the wireless network.

Redirection and Captive Portal credentials apply to HTTP traffic only. A wireless device user attempting to reach websites other than those specifically allowed in the non-authenticated filter is redirected to the allowed destinations. Most HTTP traffic outside of that defined in the non-authenticated filter is redirected.

Note



Although non-authenticated role definitions are used to assist in the redirection of HTTP traffic for restricted or denied destinations, the non-authenticated filter is not restricted to HTTP operations. The filter definition is general. Any traffic, other than HTTP, that the filter does not explicitly allow is discarded by the controller.

The non-authenticated filter is applied to sessions until they successfully complete authentication. The authentication procedure results in an adjustment to the user's applicable Policy Rule for the access role.

Typically, default filter ID access is less restrictive than a non-authenticated profile. It is the administrator's responsibility to define the correct set of access privileges.

Note



Administrators must ensure that the non-authenticated filter allows access to the corresponding authentication server:

- **Internal Captive Portal** — IP address of the VNS interface
 - **External Captive Portal** — IP address of external Captive Portal server
-

Non-authenticated Role Examples

The following table lists the rules that a basic non-authenticated role for internal Captive Portal should have, in the specified order:

Table 35: Non-authenticated Role Example A

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the captive portal	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		****	Default access control action is to deny all.

**Note**

For external Captive Portal, an additional rule to Allow (in/out) access to the external Captive Portal authentication/web server is required.

If you place URLs in the header and footer of the Captive Portal page, you must explicitly allow access to any URLs mentioned in the authentication server's page, such as:

- **Internal Captive Portal** — URLs referenced in a header or footer
- **External Captive Portal** — URLs mentioned in the page definition

The following table is another example of a non-authenticated filter that adds additional policy rules. The additional rules do the following:

- Deny access to a specific IP address.
- Allow only HTTP traffic.

Table 36: Non-authenticated Role Example B

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the default gateway	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific IP address range (such as:0/24).
x	x	x	***.80	Allow all port 80 (HTTP) traffic.
x	x		****	Default access control action is to deny all.

Once a wireless device user has logged in on the Captive Portal page and has been authenticated by the RADIUS server, then the following rules apply:

- **Role filters** — If a filter ID associated with this user is returned by the authentication server, then the Role with the same name as the filter ID will be applied.
- **Default filter** — If no matching filter ID is returned from the authentication server.

Authenticated Rules Examples

Here are examples of possible policy rules for authenticated users. The following table disallows some specific access before allowing everything else.

Table 37: Policy Rules Example A

In	Out	Allow	IP / Port	Description
x	x		*.*.*:22-23	SSH sessions
x	x		192.168.18.0/24	Deny all traffic to a specific IP address or address range
x	x	x	*.*.*.	Default action is to allow everything else

The following table allows some specific access and denies everything else.

Table 38: Policy Rules Example B

In	Out	Allow	IP / Port	Description
x	x	x	192.168.18.0/24	Allow traffic to a specific IP address or address range.
x	x		*.*.*.	Default action is to deny all.

Policy Rules for a Default Role

After authentication of the wireless device user, the default filter applies only after the following conditions are met:

- No filter ID attribute value is returned by the authentication server for this user.
- No Role match is found on the controller for the filter ID value.

The final rule in the default filter should be a catch-all rule for any traffic that did not match a filter. A final 'Allow All' rule in a default filter ensures that a packet is not dropped entirely if no match is found. VNS Role is also applicable for Captive Portal and MAC-based authorization.

Default Role Examples

The following are examples of policy rules for a default filter:

Table 39: Default Role Examples

In	Out	Allow	IP / Port	Description
x	x		192.168.18.0/24	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to Web browsing
x	x		192.168.18.10	Deny all access to a specific IP
x	x	x	*.*.*.	Default access control action is to allow or contain to VLAN
	x		Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to Web browsing the host
x			10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as FTP (port 21)
	x	x	10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network

Table 39: Default Role Examples (continued)

In	Out	Allow	IP / Port	Description
x		x	10.3.0.20	Allow all other traffic from Intranet network to wireless devices
x	x		*.*.*.*	Default action is to deny/drop

Policy Rules Between Two Wireless Devices

Traffic from two wireless devices that are on the same VNS and that are connected to the same AP will pass through the controller and therefore be subject to a filtering role. You can set up policy rules that allow each wireless device access to the default gateway, but also prevent each device from communicating with each other.

Add the following two rules to a filter, before allowing everything else:

Table 40: Rules Between Two Wireless Devices

In	Out	Allow	IP / Port	Description
x	x	x	10.3.2.25	Allow access to the Gateway IP address of the VNS only
x	x		10.3.5.28.0/24	Deny all access to the VNS subnet range (such as 0/24)
x	x	x	*.*.*.*	Default access control action is contain to VLAN.

**Note**

You can also prevent the two wireless devices from communicating with each other by setting Block Mu to MU traffic. See [Configuring a Basic WLAN Service](#) on page 274.

Defining Policy Rules for Wireless APs

You can also apply policy rules on the wireless AP. Applying policy rules at the AP helps restrict unwanted traffic at the edge of your network. All APs support 64 rules. Filtering at the AP can be configured with the following Topology types:

- **Bridge Traffic Locally at the AP** — If filtering at the AP is enabled on a Bridge Traffic Locally at the AP topology, the filtering is applied to traffic in both the inbound and outbound direction, the inbound direction is from the wireless device to the network, and the outbound direction is from the network to the wireless device.
- **Routed and Bridge Traffic Locally at the EWC** — If filtering at the AP is enabled on a Routed or Bridge Traffic Locally at the EWC topology, the filtering is applied only to traffic in the inbound direction. The filters applied in the outbound direction at the AP can be the same as or different from filters applied at the controller.

A role can use more than one topology and more than one type of topology. If a role uses at least one Bridged at AP topology, the AP filters all inbound traffic assigned to the rule. The controller performs all outbound filtering.

Configuring Policy Rules

From the Policy Rules tab, create and work with the policy rules for a role. If you do not define policy rules for a role, then the role's default action is applied to all traffic subject to the role.

To configure policy rules:

- 1 Navigate to the **Policy Rules** tab. (Click **VNS > Roles > Policy Rules**.)
By default, the **Rules** tab appears, displaying a list of Policy Rules for the Role.
- 2 You can take the following actions:
 - **Add**
 - **Edit**
 - **Delete**
 - **Up**
 - **Down**
 - **Top**
 - **Bottom**

For information about adding or editing a rule, see [Understanding the Filter Rule Definition Dialog](#) on page 257.

Related Links

[Configuring a Captive Portal on an AP](#) on page 196

[Rule-Based Redirection](#) on page 244

Understanding the Policy Rules Tab

The **Policy Rules** tab displays the authentication policy rules for a user role. If you do not define policy rules for a role, then the role's default action is applied to all traffic subject to the role.

VLAN & Class of Service
Policy Rules

Inherit filter rules from currently applied role i

Rules
 AP Filtering
 Custom AP Rules

Action	Name	Protocol	QoS	In	Out
Deny	0.0.0.0/0	Any	None	dest	none
Deny	0.0.0.0/0	Any	None	none	src

Add
Edit
Delete
Up
Down
Top
Bottom

Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters instead.

Figure 52: Policy Rules Tab

Table 41: Policy Rules Tab - Fields and Buttons

Field/Button	Description
Inherit policy rules from currently applied role	Select if you do not want to apply new filter settings. If you do not apply new filter settings, the wireless client uses filter settings from a previously applied role. If rules were never defined, then the system enforces the rules from the Global Default Policy. If you choose to apply new filter settings by not selecting this option, the new filter settings will overwrite any pre-existing filter settings.
"Allow" action in policy rules contains to the VLAN assigned by the role	<p>Note: This option only appears on roles that have been upgraded to 8.31 or later from a previous release and on new roles that have custom AP filtering enabled.</p> <p>The flag is provided for backward compatibility. The administrator can achieve the same effect by modifying each rule with an "Allow" action to "Contain to VLAN" where the containment VLAN is the one referenced by the role's default access control action. When enabled, the "Allow" action forwards the packet on the VLAN of the assigned topology of the containing policy. If the policy does not have a default topology, a series of decision rules are applied to decide which topology the packet was forwarded on. When disabled, the "Allow" action in policy rules is interpreted as "contain to PVID".</p>

Table 41: Policy Rules Tab - Fields and Buttons (continued)

Field/Button	Description
AP Filtering	Select to apply the configured rules to the AP.
Custom AP Rules	Select to create a new filter definition to apply to the AP.
Rules/Custom AP rules Tab	
Action	Identifies the access control.
Name	Displays the IP address and port to which this policy rule applies.
Protocol	Displays the applicable protocol.
QoS	Indicates if the rule has QoS enabled. Policy-enabled QoS is a network service that provides the ability to prioritize different types of traffic and to manage bandwidth over a network.
In	Identifies the rule that applies to traffic from the wireless device that is trying to get on the network. You can change this setting using the drop-down menu. Options include: <ul style="list-style-type: none"> • Source (src) • None • Both - available in Advanced Filtering Mode only
Out	Identifies which IPv4 address field is matched by the rule when applied in the outbound direction (toward the wireless device.) You can change this setting using the drop-down menu. Options include: <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>The role for outbound traffic may be impacted by the selection (mode) for Egress Filtering. For more information, see Configuring Egress Filtering Mode on page 362.</p>
Add	Click to add a new rule. The Filter Rule Definition dialog displays. See Understanding the Filter Rule Definition Dialog on page 257.
Edit	Click to edit the selected definition. See Understanding the Filter Rule Definition Dialog on page 257.
Delete	Click to delete the rule.
Up, Down, Top, Bottom	Select a rule and click to either move the rule up or down in the list, or move the rule to the top of the list. The policy rules are executed in the order in which you define them.
Save	Click to save the configuration.

Custom AP Rules

In general, an AP that performs filtering should apply the same set of policy rules for a role as the controller. However, this is not mandatory. An AP can enforce a different set of rules than the controller.

In general, avoid using Custom AP filters. Custom AP filters are provided primarily for backward compatibility. For example, they are useful when using policies that have more than 32 rules.

There are restrictions on a role that uses custom AP filtering, including the following:

- Custom Rules option is not visible when L7 filter rules are present.
- The role cannot use Layer 2 filter rules.
- The role cannot use 'Contain to VLAN' actions in rules.
- The role's default action must be 'Contain to VLAN' or 'No Change'.
- The role's static untagged egress VLAN list must be empty.

Related Links

[Creating a Custom AP Filter](#) on page 257

[Understanding the Filter Rule Definition Dialog](#) on page 257

Creating a Custom AP Filter

To create a custom AP filter:

- 1 Click **VNS > Roles > Policy Rules** and select the **AP Filtering** checkbox.



Note

The AP Filtering option is not available when L7 filters are present. For more information, see [Configuration Rules with L7 Filters](#) on page 262.

The Custom AP Rules checkbox appears.

- 2 Select the **Custom AP Rules** checkbox.

The **Custom AP Rules** tab appears.

- 3 Click the **Custom AP rules** tab.

- 4 You can take the following actions:

- **Add**
- **Edit**
- **Delete**
- **Up**
- **Down**
- **Top**
- **Bottom**

For information about adding or editing a rule, see [Understanding the Filter Rule Definition Dialog](#) on page 257.

Related Links

[Custom AP Rules](#) on page 256

[Understanding the Filter Rule Definition Dialog](#) on page 257

Understanding the Filter Rule Definition Dialog

Define filter rules from the [Figure 53](#). This dialog displays when you click **Add** or **Edit** from the **Rules** tab or from the **Custom AP Rules** tab.

Figure 53: Filter Rule Definition Dialog

Table 42: Filter Rule Definition Dialog - Fields and Buttons

Field/Button	Description
Classification	Select Layers 2-4 to display configuration options for the data link, routing, and transport layers. Select Layer 7 to configure options related to the application layer. For more information, see Layer 7 configuration .
Direction	

Table 42: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
In Filter	In the drop-down menu, select which IPv4 addresses in the IP header to match for traffic flowing from the station to the network. Options include: <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only
Out Filter	In the drop-down menu, select which IPv4 addresses in the IP header to match for traffic flowing from the network to the station. Options include: <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>The role for outbound traffic rules may be impacted by the selection (mode) for Egress Filtering. For more information, see Configuring Egress Filtering Mode on page 362.</p>
Classification - Layer 2, 3, 4	
Ethertype	Select a matching Ethertype filter for the selected policy rule. <p>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 .</p>
Mac Address	Select Any MAC or User Defined and provide the Mac Address.
Priority	Select a Priority from the drop-down list.
IP/subnet	Select one of the following: <ul style="list-style-type: none"> • User Defined, then type the destination IP address and mask. Use this option to explicitly define the IP/subnet aspect of the rule. • IP - select to map the rule to the associated Topology IP address. • Subnet - select to map the rule to the associated Topology segment definition (IP address/mask).
Port	From the Port drop-down list, select one of the following: <ul style="list-style-type: none"> User Defined, then type the port number. Use this option to explicitly specify the port number. A specific port type. The appropriate port number or numbers are added to the Port text field.
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
ToS/DSCP	Select the ToS/DSCP value to match, if any, to define the Layer 3, 4 ToS/DSCP bits. Enter a hexadecimal value in the 0x (DSCP:) field.
Select	Click the Select button to open the ToS/DSCP Configuration dialog. For more information, see Priority and ToS/DSCP Marking on page 443.

Table 42: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Mask	This is a mask for the ToS/DSCP field match. The mask allows the match to be based on specific bits in the ToS/DSCP match value. Enter a hexadecimal value.
Application	
Application	<p>Select from one of the following pre-defined IDs to support L5+ filtering:</p> <ul style="list-style-type: none"> • None • Link Local Multicast Name Resolution Query • Link Local Multicast Name Resolution Response • Simple Service Discovery Protocol Query • Simple Service Discovery Protocol Unsolicited Announcement • mDNS-SD Query • mDNS-SD Response
Action	
Access Control	<p>Select from one of the following:</p> <ul style="list-style-type: none"> • None - No role defined. • Allow - Packets contained to role's default action's VLAN/topology. • Deny - Any packet not matching a rule in the policy is dropped. • Containment VLAN - A topology to use when a VNS is created using a role that does not specify a topology. • HTTP Redirect - Indicates redirect action. <p>Rule-based Redirection is explicit when the redirection flag is enabled and a rule is defined for redirection. The redirection destination can be defined on the role or as part of a WLAN Service configuration. If a redirection destination is not configured, the default destination is 'Own WLAN', which indicates the WLAN of the device. Redirection is allowed on any port.</p> <p>For more information about Rule-based Redirection, see Rule-Based Redirection on page 244.</p> <p>Note: Access control option "Contain to VLAN" and "Redirect" are not supported for L7 rules.</p>
Class of Service	<p>Select an existing class of service from the drop-down list. For information about how to configure a Class of Service, go to Classes of Service Overview on page 439.</p>

Table 42: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Traffic Mirror	<p>When enabled, this option sends a copy of the network packets to a mirroring L2 port for analysis, in an effort to monitor network traffic. The Purview Engine analyses the traffic, and the assigned port can only be used for traffic analysis.</p> <p>You can enable traffic mirroring from the WLAN Service, from the Role, or from the Filter Rule. Setting traffic mirroring at the Filter Rule takes precedence over settings for the Role and WLAN Service. The order of precedence for the traffic mirror setting is: Filter Rule, Role, WLAN Service. To set the port number, go to VNS > Global > Netflow/MirrorN Configuration.</p> <p>Valid values for Filter Rule and Role are:</p> <ul style="list-style-type: none"> • None - No traffic mirroring • Enable - Traffic mirroring enabled. Traffic is copied if the filter rule matches or the role is applied. • Prohibited - Traffic mirroring is prohibited for this role. Traffic is not copied when the filter rule matches or the role is applied. <p>Valid values for the WLAN Service are:</p> <ul style="list-style-type: none"> • Prohibited - Traffic is not copied for this WLAN Service. • Enable in both directions - Traffic coming from wireless clients and traffic targeted at specific clients is copied. • Enable in direction only - Traffic generated by wireless clients only is copied.
OK	Click to add the rule to the filter group. The information is displayed in the role rule table.
Cancel	Click Cancel to discard your changes.

Related Links

[L7 Configuration](#) on page 262

[Rule-Based Redirection](#) on page 244

[Configuring Policy Rules](#) on page 254

[Configuring a Captive Portal on an AP](#) on page 196

DPI L7 Configuration Restrictions

The Deep Packet Inspection (DPI) engine runs independently on the controller and on selected AP models (AP38xx and AP39xx). The DPI engine that is used depends on the underlying topology of the role. The controller DPI handles traffic for centralized topologies (Bridged@Controller and Routed) for traffic in both directions. The AP's DPI handles distributed topologies (Bridged@AP).

Enabling “App Visibility” in the WLAN causes end-user traffic of the particular WLAN to be sent to and processed by the respective DPI engine. For DPI and L7 filters to work, each instance of the DPI engine running on the AP or on the controller must inspect traffic that is moving in both directions of the connection.

The mixed topologies (B@AP & tunneled in same role) are not supported, and are disabled in the user interface, when L7 application rules are defined in a role. As a result, the “Contain to VLAN” Action option is unavailable for configuration of an L7 Application Rule.

For more information, see [Configuration Rules with L7 Filters](#) on page 262.

Related Links

[Configuration Rules with L7 Filters](#) on page 262

[L7 Configuration](#) on page 262

Configuration Rules with L7 Filters

The controller imposes the following L7 filter configuration rules:

- Rule #1 – If L7 filter rules are configured, “AP filter” and “custom AP filter” in Roles is disabled and the corresponding checkbox options are hidden.

This allows the Configuration Manager to configure the system for upstream filtering at the controller, if possible, with no mixed B@AC and B@AP configuration within a role - enforced by [Rule # 3](#).

- Rule # 2 – Access control options “Contain to VLAN” and “Redirect” are not supported for L7 rules.

For DPI to identify a flow, TCP packets (3- way handshake exchanges and initial payload packets) must be allowed to pass through the system. If after the traffic flow is classified and the system diverts the rest of the traffic flow to a different VLAN (and most likely to a different server), then the new server treats the packets as stray traffic. This is because the new server did not exchange a 3- way handshake with the client for the connection.

- Rule # 3 – Configuration Manager (CM) checks overall configuration as configuration is entered.

If CM detects mixed B@AC and B@AP rules in the same role, and the role has L7 filter rules, then the configuration is rejected.

- Rule # 4 – For L2/L3/L4 rule configuration, if COS is configured, the GUI prompts users to set “AP filter”. But, if L7 rules are present, then the GUI will always disable the AP filter option. See [Rule # 1](#)).

L7 Configuration

Define Layer 7 filter rules. This dialog displays when you select **L7** on the **Filter Rule Definition** dialog.

Use this dialog to configure filters that allow or deny specific applications or application groups from running on the network, and specify class of service and traffic mirroring.

Figure 54: L7 Properties - Filter Rule Definition Dialog

Table 43: Filter Rule Definition Dialog - Fields and Buttons

Field/Button	Description
Classification	Select Layer 7 to configure options related to the application layer. For more information about layers 2-4, see Understanding the Filter Rule Definition Dialog on page 257.
Direction	
In Filter	Select which IPv4 addresses in the IP header to match for traffic flowing from the station to the network. Options include: <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only

Table 43: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Out Filter	<p>Select which IPv4 addresses in the IP header to match for traffic flowing from the network to the station. Options include:</p> <ul style="list-style-type: none"> • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only <p>The role for outbound traffic rules may be impacted by the selection (mode) for Egress Filtering. For more information, see Configuring Egress Filtering Mode on page 362.</p>
Application	
Application Search	Type the application to search for. The Group and Name fields are automatically populated when you select an application from the Search field.
Group	Internet applications are organized in groups based on the type or purpose of the application. Once you select an Application Group, the Name drop-down is populated with application names that are part of the specified group. See Application Groups on page 265.
Name	Names of applications that are a member of the specified group.
Custom Web Applications	You can include custom applications in the Filter Rule Definition dialog. For more information, see Including Custom Apps on page 268.
Note: A role can be configured with application visibility rules and rules referencing IPv6 classifiers, but the application visibility rules are ignored for http[s] flows over IPv6. They will continue to apply to flows over IPv4.	
Action	

Table 43: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Access Control	<p>Select from one of the following:</p> <ul style="list-style-type: none"> • 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 policy is dropped. • Containment VLAN - A topology to use when a VNS is created using a role that does not specify a topology. <p>Note: Do not specify a VLAN with a Routed topology if the IPv6 classifier is used. IPv6 classifiers are not supported on a Routed topology.</p> <ul style="list-style-type: none"> • HTTP Redirect - Indicates redirect action. <p>Rule-based Redirection is explicit when the redirection flag is enabled and a rule is defined for redirection. The redirection destination can be defined on the role or as part of a WLAN Service configuration. If a redirection destination is not configured, the default destination is 'Own WLAN', which indicates the WLAN of the device. Redirection is allowed on any port.</p> <p>For more information about Rule-based Redirection, see Rule-Based Redirection on page 244.</p>
Class of Service	<p>Select an existing class of service from the drop-down list. For information about how to configure a Class of Service, go to Configuring Roles on page 240.</p>
Traffic Mirror	<p>Select from one of the following:</p> <ul style="list-style-type: none"> • None - No rule defined • Enable - Default setting • Prohibited - Traffic Mirroring prohibited for this Filter Rule.
OK	<p>Click to add the rule to the filter group. The information is displayed in the role rule table.</p>
Cancel	<p>Click Cancel to discard your changes.</p>

Related Links

[DPI L7 Configuration Restrictions](#) on page 261

[Configuration Rules with L7 Filters](#) on page 262

[Application Groups](#) on page 265

[Allowing for Restricted Sets of Applications and Resources](#) on page 266

[Host Name DNS Support](#) on page 267



Application Groups

- Advertising
- Business Applications
- Certificate Validation
- Cloud Computing
- Cloud Storage
- Corporate Website
- Databases
- E-commerce
- Education
- Finance
- Games
- Health Care
- Location Services
- Mail
- News and Information
- Peer to Peer
- Protocols
- Real Time and Cloud Communications
- Restricted Content
- Search Engines
- Social Networking
- Software Updates
- Sports
- Storage
- Streaming
- Travel
- VPN and Security
- Web Applications
- Web Collaboration
- Web Content Services
- Web File Sharing
- All

ExtremeWireless Special Purpose Groups

- Unknown Apps
- Wild Card



Allowing for Restricted Sets of Applications and Resources

With the use of two new groups: the Unknown Apps group and the Wild Card group, you can configure policy filters that improve application control. Defined signature rules allow fine-tuning of how to handle traffic for specific applications or traffic categories.

The Unknown Apps group allows you to take action on applications that the Deep Packet Inspection (DPI) sensor does not recognize. When the DPI sensor fails to classify a flow, the flow is automatically considered unknown and it is classified as part of the Unknown Apps group. You can assign standard actions (allow, deny, rate limit, etc) to flows belonging to the Unknown Apps group.

The Wild Card group makes it simple to allow access to restricted sets of applications and resources. When configuring filters for restrictive sets:

- 1 Configure the Allowed application filters first.
- 2 Configure a Deny filter specifying the Group = **Wild Card** and Name = **All**.
- 3 Configure a Deny filter specifying Group = **Unknown Apps** and Name = **All**.



Host Name DNS Support

When redirecting to an external captive portal (ECP), you can permit end users to log in with their credentials from a third-party site. ExtremeWireless builds a dynamic list of server addresses for sites by monitoring the DNS replies between DNS servers and the mobile user.

Configure an Allow filter rule that applies to all learned server addresses for a specific site.

Related Links

[DNS Resolution](#) on page 267

[Configuring a Host Name Rule](#) on page 267

DNS Resolution

The controller and AP handle DNS resolution (mapping of the host name to an IP address) at runtime for third-party login support. DNS resolution is handled by the AP for B@AP topologies and handled by the controller for B@AC and Routed topologies.

First, configure a host name pattern in the Custom Application dialog as part of the Layer 7 filter configuration. The ExtremeWireless data plane inspects DNS replies for host name patterns that match the user-configured patterns. When a match is found, the host name IP pair is stored in the database. The data plane only considers the user-configured patterns when inspecting the DNS reply.

For example, the pattern `facebook.com` matches any string that ends with “facebook.com”. Valid matches include `any.facebook.com` and `1.any.2.facebook.com`. Patterns that do *not* match include: `facebook.org.com`.

A single host name supports multiple IP addresses. The data plane reserves space for up to 128 IP addresses per host name.

Configuring a Host Name Rule

DNS-based rules are defined as custom L7 signatures. ExtremeWireless matches the defined pattern to the corresponding IP address. Take the following steps to configure a rule that allows mobile clients to authenticate using credentials from a specific host.

- 1 Go to **VNS > Roles > Policy Rules** and click **Add**.

- 2 Create a new filter definition. For more information, see [Understanding the Filter Rule Definition Dialog](#) on page 257.
- 3 On the **Filter Rule Definition** dialog, select the **L7** radio button.
- 4 Select the link **Custom Web Applications**.
- 5 Click the plus button and configure the parameters on the **Custom Web Application** dialog.
Specify Type = **Host name**. The Host Name type differentiates the definition from other extended signatures.

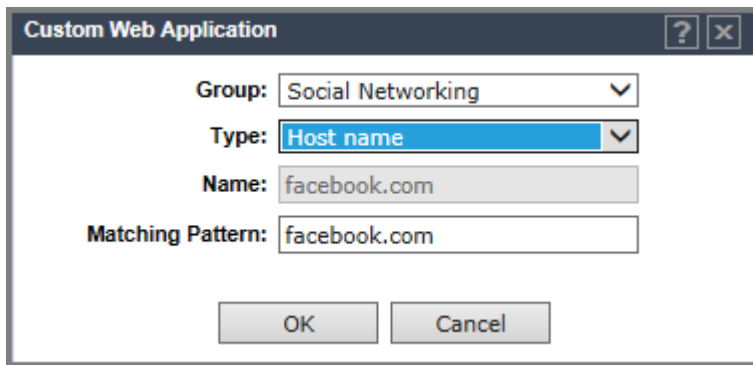


Figure 55: Host Name Rule Configuration

Custom Apps List

Use the custom web application definition editor to define the characteristics of traffic fingerprints used for Deep Packet Inspection and Layer 7 policy enforcement. To add or remove custom Apps from the **Filter Rule Definition** dialog:

- 1 Select **Custom Web Applications**.
- 2 To add an App, click the plus sign. See [Including Custom Apps](#) on page 268.
- 3 To remove an App, select the App and click the minus sign.
- 4 Click **OK**.

Related Links

[Understanding the Filter Rule Definition Dialog](#) on page 257

[L7 Configuration](#) on page 262

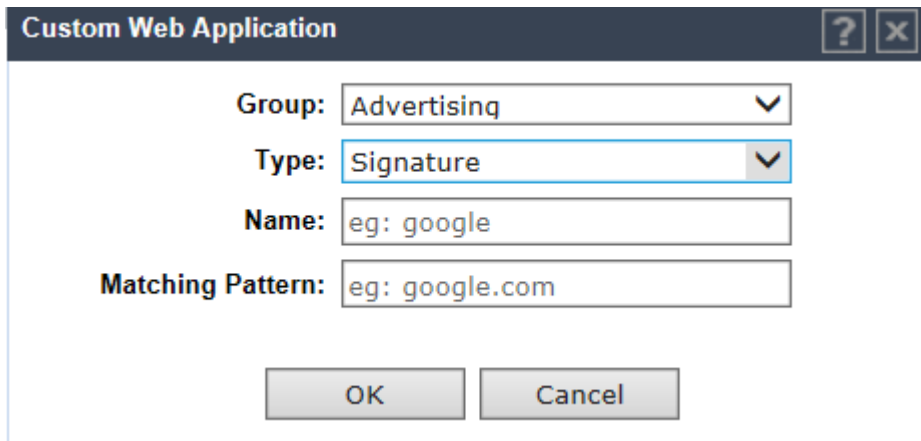
[Including Custom Apps](#) on page 268

Including Custom Apps

To add custom apps to the **L7 Filter Rule Definition** dialog:

- 1 From the **Filter Rule Definition** dialog, select **L7**.
- 2 Click **Custom Web Application**.

- 3 Click the plus sign and enter the following:
 - **Group.** The group names are pre-defined standard Extreme Application Analytics™ signature groups. The group names are case-sensitive.
 - **Type.** Type of authentication. Valid values are:
 - **Signature.** Standard IP address sent in Signature.
 - **Layer 3 host name.** Authentication based on User Defined IP/subnet parameter in Layer 3 configuration. You can define up to 64 host name patterns per controller or site. For more information, see [Host Name DNS Support](#) on page 267.
 - Enter a Matching Pattern. The Matching Pattern is the URL pattern that is associated with the application (case sensitive, up to 64 characters).
 - After entering the Matching Pattern, the Name value is automatically provided.



Custom Web Application [?] [X]

Group: Advertising

Type: Signature

Name: eg: google

Matching Pattern: eg: google.com

OK Cancel

Figure 56: Adding Custom Web Applications

4. Click **OK**.

The **Custom Web Application** list displays.

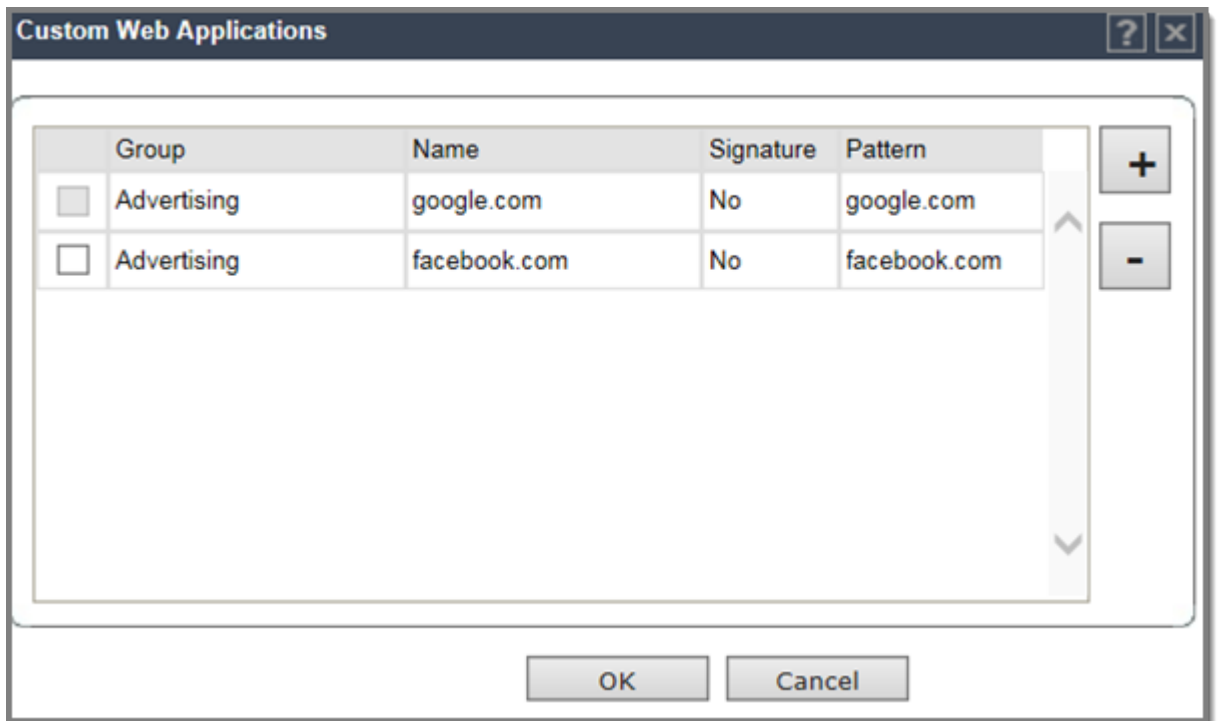


Figure 57: Custom Web Applications list

- 5 Select the checkbox and click **OK** to add the custom app to the Name drop-down field on the **L7 Configuration** dialog.

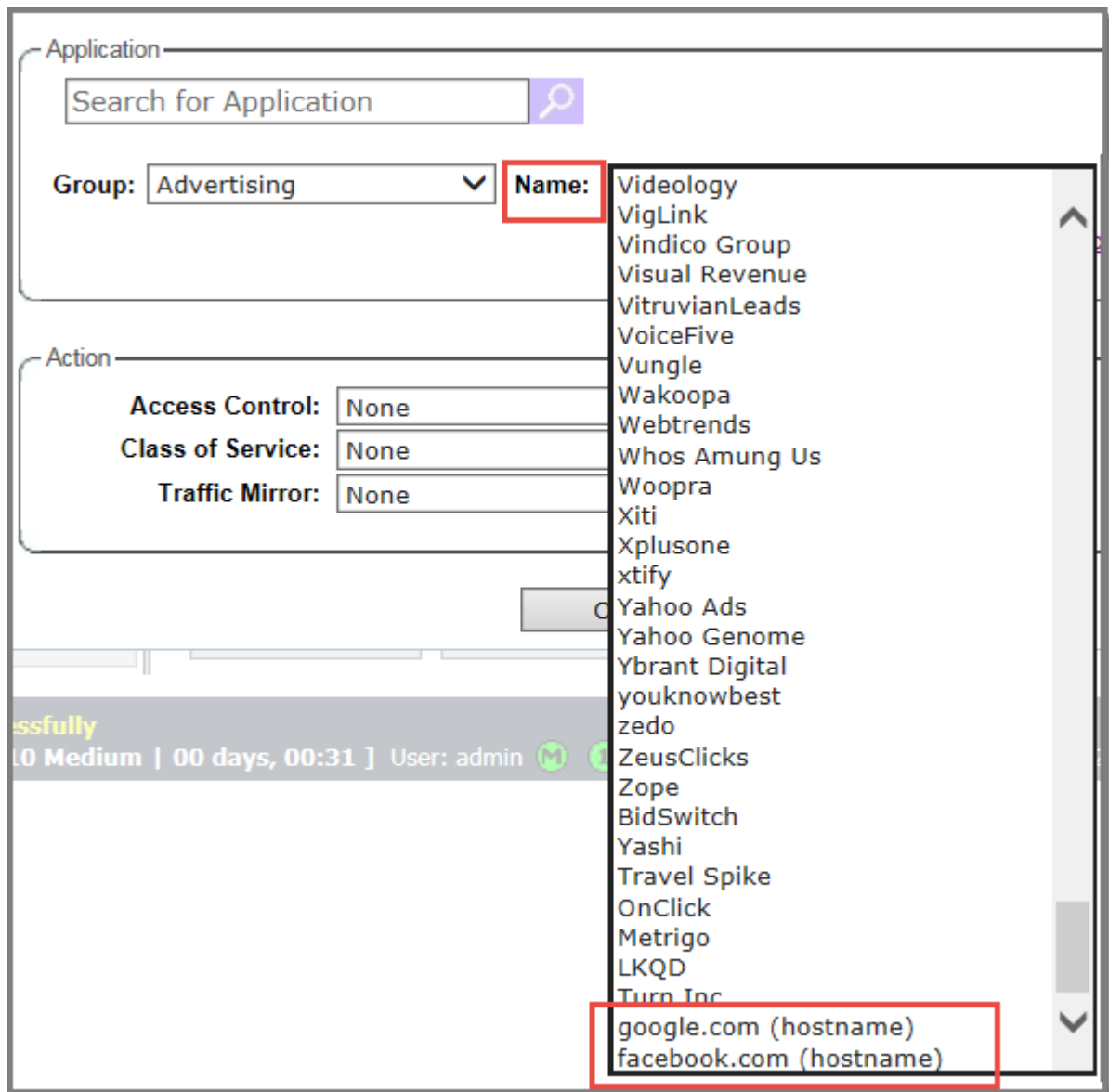


Figure 58: L7 Configuration: Custom Apps with hostname rule

Related Links

[Application Groups](#) on page 265

[Host Name DNS Support](#) on page 267

Partially Specified Policy

A partially specified policy is one that has “No change” selected for filters, default topology, or default qos. When two policies are applied to a station and one of them is “partially specified”, the “No change” settings are overwritten by the settings of the other policy. When a station successfully authenticates

and is assigned a partially specified policy, the “No change” elements of the policy are replaced with the corresponding elements of the WLAN Service’s default authenticated policy.

Consider the following example. Suppose a VNS is defined that uses policy P1 for its default non-authenticated policy and policy P2 for its default authenticated policy. Policy P1 assigns the station to topology T1 and policy P2 assigns the station to topology T2. Suppose there is a policy P3, which has “No change” set for its topology.

A client on the VNS will be assigned to P1 with topology T1 when he first associates to the VNS. Now suppose the station is assigned P3 by the RADIUS server when the station authenticates. Even though the station is on T1 and P3 has no change set for the topology, the station will be assigned to T2. When the client is authenticated, internally on the controller, the client is first assigned to P2 then P3 is applied.

A similar scenario exists when the hybrid mode policy feature is set to use tunnel-private-group-id to assign both policy and topology but for some reason the VLAN-id-to-Policy mapping table does not contain a mapping for the returned tunnel private group id. In this case a station that successfully authenticates would be assigned the filters and default QoS of the WLAN Service’s default authenticated policy and the topology with the VLANID contained in the Tunnel-Private-Group-ID of the ACCESS-ACCEPT response.

If this is not the desired behavior, then consider the following:

- Avoid using partially specified policies.
- When the controller is configured to map the VLAN ID in the Tunnel-Private-Group-ID response to a policy using the mapping table, ensure that there is a policy mapping for each VLAN ID that can be returned to the controller by the RADIUS server.

7 Configuring WLAN Services

WLAN Services Overview

Third-party AP WLAN Service Type

Configuring a Basic WLAN Service

Configuring Privacy

Configuring Accounting and Authentication

Configuring QoS Modes

Configuring Hotspots

WLAN Services Overview

A WLAN Service represents all the RF, authentication and QoS attributes of a wireless access service. The WLAN Service can be one of the following types:

- Standard — A conventional service. Only APs running Extreme Networks ExtremeWireless software can be part of this WLAN Service. This type of service may be used as a Bridged @ Controller, Bridged @ AP, or Routed VNS. This type of service provides access for mobile stations. Therefore, roles can be assigned to this type of WLAN service to create a VNS.
- Third Party AP — A wireless service offered by third party APs. This type of service provides access for mobile stations. Therefore, roles can be assigned to this type of WLAN service to create a VNS.
- Dynamic Mesh and WDS (Static Mesh)— A group of APs organized into a hierarchy for the 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 remote service should have the same SSID name and privacy as the home remoteable service. Any WLAN Service/VNS can be a remoteable service, though deployment preference is given to tunneled topologies (Bridged@Controller and Routed).

To reduce the amount of information distributed across the mobility domain, you will explicitly select which WLAN Services are available from one controller to any other controller in the mobility domain.

The WLAN Service remoteable property is synchronized with the availability peer, making the WLAN service published by both the home and foreign controllers.

The following types of authentication are supported for remote WLAN services:

- None
- Internal/External Captive Portal
- Guest Portal

- Guest Splash
- AAA/802.1x

Third-party AP WLAN Service Type

For more information, see [Working with Third-party APs](#) on page 515.

A third-party AP WLAN Service allows for the specification of a segregated subnet by which non-Extreme Networks ExtremeWireless APs are used to provide RF services to users while still utilizing the controller for user authentication and user role enforcement.



Note

Third-party AP devices are not fully integrated with the system and therefore must be managed individually to provide the correct user access characteristics.

The definition of third-party AP identification parameters allows the system to be able to differentiate the third-party AP device (and corresponding traffic) from user devices on that segment. Devices identified as third-party APs are considered pre-authenticated, and are not required to complete the corresponding authentication verification stages defined for users in that segment (typically Captive Portal enforcement).

In addition, third-party APs have a specific set of filters (third-party) applied to them by default, which allows the administrator to provide different traffic access restrictions to the third-party AP devices for the users that use those resources. The third-party filters could be used to allow access to third-party APs management operations (for example, HTTP, SNMP).

Configuring a Basic WLAN Service

To configure a WLAN service:

- 1 Go to **VNS>WLAN Services**.

The screenshot shows the VNS configuration interface for WLAN Services. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A sidebar on the left contains a tree view with categories: New..., Global, Sites, Virtual Networks, and WLAN Services (selected). Under WLAN Services, various service IDs are listed, such as CNL-218-0-0 through CNL-218-WDS. The main content area displays a table of WLAN Services with columns for Name, Type, Enabled, SSID, Privacy, Auth. Mode, and Radio Mode. Below the table are 'New' and 'Delete Selected' buttons. A red warning message is present below the table.

Name	Type	Enabled	SSID	Privacy	Auth. Mode	Radio Mode
<input type="checkbox"/> CNL-218-0-0	Standard	✓	CNL-218-0-0-ssid	WEP	Internal Captive Portal	a/n/ac
<input type="checkbox"/> CNL-218-0-1	Standard	✓	CNL-218-0-1-ssid	WPA-PSK	External Captive Portal	a/n/ac
<input type="checkbox"/> CNL-218-0-2	Standard	✓	CNL-218-0-2-ssid	None	Disabled	a/n/ac
<input type="checkbox"/> CNL-218-0-3	Standard	✓	CNL-218-0-3-ssid	Dyn. Keys (WEP)	802.1x	a/n/ac
<input type="checkbox"/> CNL-218-1-2-wds	Standard	✓	CNL-218-1-2-wdsChildsWiE	WPA	802.1x	a/n
<input type="checkbox"/> CNL-218-1-4-wds	Standard	✓	CNL-218-1-4-wdsChildsWiE	WPA	802.1x	a/n
<input type="checkbox"/> CNL-218-1-5	Standard	✓	CNL-218-1-5-ssid	WPA-PSK	Guest	a/n/ac

Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.

Figure 59: Configuring a WLAN Service

- 2 Click **New** to create a new service.

The screenshot shows the 'WLAN Services' configuration page. The sidebar on the left lists various network categories, with 'WLAN Services' selected. The main panel is titled 'WLAN Services' and contains a 'Core' section with the following fields:

- Name:** An empty text input field.
- Service Type:** A group of radio buttons with options: Standard (selected), WDS, Mesh, Third Party AP, and Remote.
- SSID:** An empty text input field.
- Hotspot:** A dropdown menu currently set to 'Disabled'.

Below the 'Core' section is a 'Status' section with two checked checkboxes:

- Synchronize:** . Below it, red text reads: 'Replicated when Synchronize Configuration is enabled'.
- Enable:** .

A 'Save' button is located at the bottom right of the configuration area.

Figure 60: New WLAN Service

- a Enter a name for the WLAN service.
- b Select the service type.
- c Change the SSID (optional).
- d Enable Hotspot functionality (optional). For more information, see [Configuring Hotspots](#) on page 329.
- e The default status of the WLAN service is Synchronized and Enabled.

Synchronize — Enable automatic synchronization with its availability peer. Refer to [Using the Sync Summary](#) on page 365 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable **Synchronize**.

By default the WLAN Service is enabled. Clear this checkbox to disable the WLAN Service.
- f Click **Save**.

3 For information about fields and buttons on this page, see Table 44.

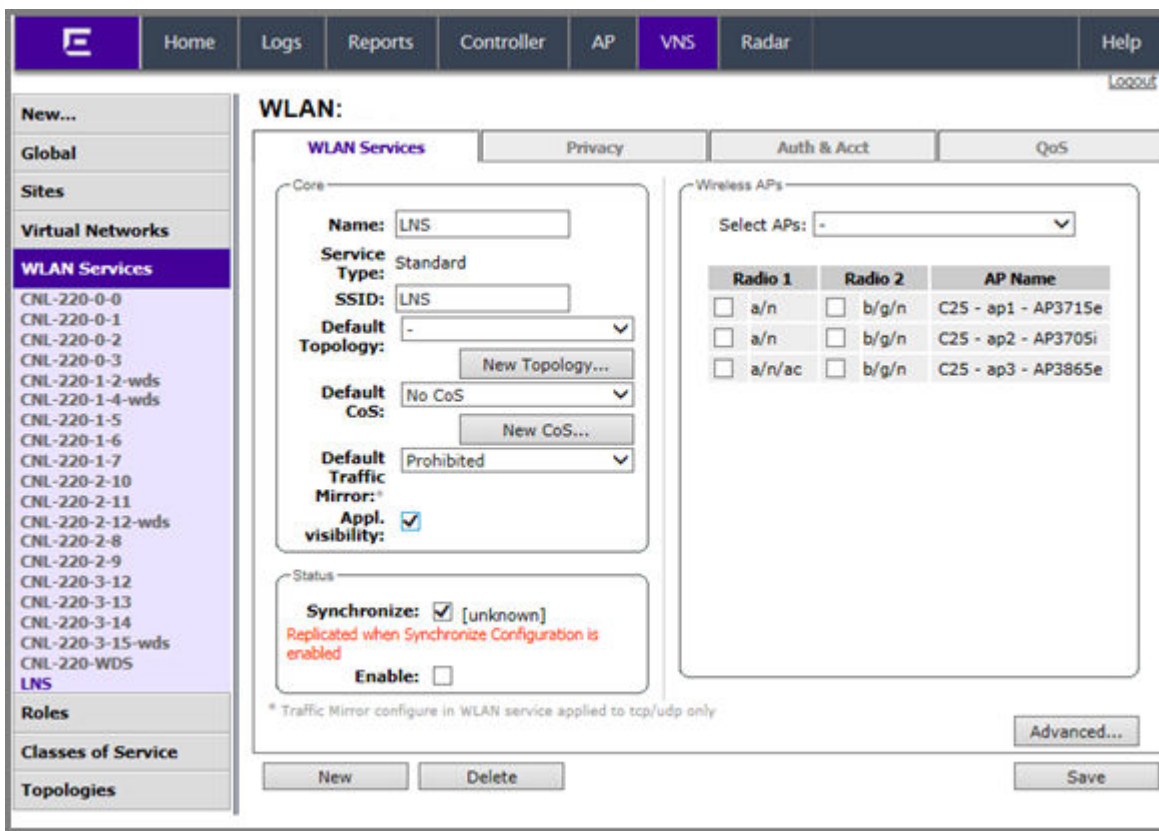


Figure 61: WLAN Service Configuration

Table 44: WLAN Services Configuration Page

Field/Button	Description
Core	
Name	Enter a name for this WLAN service
Service Type	<p>Select the type of service to apply to this WLAN service. Options include:</p> <ul style="list-style-type: none"> • Standard • WDS • Mesh • Third Party AP • Remote <p>If you selected Remote as the Service Type, select the Privacy type. If you set Service Type as either Standard or Remote, select Synchronize, in the Status area, if desired. Enabling this feature allows availability pairs to be synchronized automatically</p>
SSID	The software automatically populates this field with the WLAN service name that you supply. Optionally, you can change this. If you are creating a remote WLAN service, select the SSID of the remoteable service that this remote service will be paired with.

Table 44: WLAN Services Configuration Page (continued)

Field/Button	Description
Default Topology	<p>From the drop-down list, select a preconfigured topology, topology group, or click New Topology to create a new one. Refer to Configuring a Basic Data Port Topology on page 223 for information about how to create a new topology.</p> <p>A WLAN service uses the topology of the role assigned to the VNS, if such a topology is defined. If the role doesn't define a topology, you can assign an existing topology as the default topology to the WLAN service. If you choose not to assign a default topology to the WLAN service, the WLAN service will use the topology of the global default policy (by default, Bridged at AP Untagged).</p> <p>Note: You cannot assign a default topology to a WDS, 3rd party, or remote WLAN service.</p>
Default	<p>From the drop-down list, select a preconfigured CoS or click New CoS to create a new one. Refer to Configuring Classes of Service on page 439 for information on how to create a new CoS.</p> <p>A WLAN service uses the CoS of the role assigned to the VNS, if such a CoS is defined. If the role doesn't define a CoS, you can assign an existing CoS as the default CoS to the WLAN service. If you choose not to assign a default CoS to the WLAN service, the WLAN service will use the CoS of the global default policy (by default, Bridged at AP Untagged).</p> <p>Note: You cannot assign a default CoS to a WDS, 3rd party, or remote WLAN service.</p>
Default Traffic Mirror	<p>When enabled, this option sends a copy of the network packets to a mirroring L2 port for analysis, in an effort to monitor network traffic. The Purview Engine analyses the traffic, and the assigned port can only be used for traffic analysis.</p> <p>You can enable traffic mirroring from the WLAN Service, from the Role, or from the Filter Rule. Setting traffic mirroring at the Filter Rule takes precedence over settings for the Role and WLAN Service. The order of precedence for the traffic mirror setting is: Filter Rule, Role, WLAN Service. To set the port number, go to VNS > Global > Netflow/MirrorN Configuration.</p> <p>Valid values for Filter Rule and Role are:</p> <ul style="list-style-type: none"> • None - No traffic mirroring • Enable - Traffic mirroring enabled. Traffic is copied if the filter rule matches or the role is applied. • Prohibited - Traffic mirroring is prohibited for this role. Traffic is not copied when the filter rule matches or the role is applied. <p>Valid values for the WLAN Service are:</p> <ul style="list-style-type: none"> • Prohibited - Traffic is not copied for this WLAN Service. • Enable in both directions - Traffic coming from wireless clients and traffic targeted at specific clients is copied. • Enable in direction only - Traffic generated by wireless clients only is copied. <p>Note: Traffic Mirror configured in WLAN service applies to TCP/UDP only.</p>

Table 44: WLAN Services Configuration Page (continued)

Field/Button	Description
App Visibility	Check this option to enable Application Visibility and Application Enforcement on the specific WLAN. Application Visibility allows the controller to capture throughput and byte statistics for 31 pre-selected application groups per client. The data is refreshed every 2 minutes. Enabling this option increases CPU load. Clear this option when Application Visibility and Application Enforcement is not required.
Status	
Synchronize	Synchronize — Enable automatic synchronization with its availability peer. Refer to Using the Sync Summary on page 365 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable this feature.
Enable	The WLAN service is enabled by default, unless the number of supported enabled WLAN services has been reached. To disable the WLAN service, clear the checkbox.
Wireless APs	
Select APs	Select APs and their radios by grouping. Options include: <ul style="list-style-type: none"> • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2. • clear all selections — Click to clear all of the AP radio assignments. • original selections — Click to return to the AP radio selections prior to the most recent save. <p>Note: If two controllers have been paired for availability (for more information, see Availability on page 490), each controller's registered APs are displayed as foreign in the list of available APs on the other controller</p>
Radio 1	Assign the APs' Radios to the service by selecting the individual radios' checkboxes. Alternatively, you can use the Select APs list.
Radio 2	Assign the APs' Radios to the service by selecting the individual radios' checkboxes. Alternatively, you can use the Select APs list.

Table 44: WLAN Services Configuration Page (continued)

Field/Button	Description
Ports	<p>Supported on the AP3912. Select one or more client ports for each WLAN Service.</p> <ul style="list-style-type: none"> • A WLAN service can be assigned to one or more radios and ports. A client port can be assigned to only one WLAN service. The assignment enables the port. • One policy definition for wired and wireless users. Users on wired ports receive the same default policy. • Wireless and wired users associated to the same WLAN service and receive identical service. They are affected by the same policies and filters. • ExtremeWireless v10.21.02 limits wired port assignment to open WLAN services, MBA, and captive portal. <p>Alternatively, you can use the Select APs list. (With an AP3912.)</p>
AP Name	Displays the AP name that you assigned on the AP Properties screen.
Advanced	Click to access the WLAN service advanced configuration options. The Advanced configuration page options are described in Advanced WLAN Service Configuration on page 281.
New	Click to create a new WLAN service.
Delete	Click to delete this WLAN service.
Save	Click to save the changes to this WLAN service. If you are creating a new service, the WLAN Services configuration window is displayed, allowing you to assign APs to the service.

**Note**

If two controllers have been paired for availability each controller's registered wireless APs are displayed as foreign in the list of available APs on the other controller. For more information, see [Availability](#) on page 490.

After you have assigned an AP Radio to eight WLAN Services, it will not appear in the list for another WLAN Service setup. Each Radio can support up to eight SSIDs (16 per AP). Each AP can be assigned to any of the VNSs defined within the system.

The controller can support the following active VNSs:

- C5110 — Up to 128 VNSs
- C5210 — Up to 128 VNSs
- C4110 — Up to 64 VNSs
- C25 — Up to 16 VNs
- C35 — Up to 16 VNs
- V2110 — Up to 128 VNSs

**Note**

You can assign the Radios of all three AP variants — ExtremeWireless Appliance, Outdoor AP, and Wireless 802.11n AP — to any VNS.

Advanced WLAN Service Configuration

Table 45: Advanced WLAN Service Configuration Page

Field/Button	Description
Timeout	
Idle (pre)	Specify the amount of time in minutes that a Mobile user can have a session on the controller in pre-authenticated state during which no active traffic is passed. The session will be terminated if no active traffic is passed within this time. The default value is 5 minutes.
Idle (post)	Specify the amount of time in minutes that a Mobile user can have a session on the controller in authenticated state during which no active traffic is passed. The session will be terminated if no active traffic is passed within this time. The default value is 30 minutes.
Session	Specify the maximum number of minutes of service to be provided to the user before the termination of the session.
RF - select one or more of the following options:	
Suppress SSID	Select to prevent this SSID from appearing in the beacon message sent by the AP. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.
Enable 11h support	Select to enable 11h support. By default this option is disabled. It is recommended that you enable this option.
Apply power reduction to 11h clients	Select to enable the AP to use reduced power (as does the 11h client). By default this option is disabled. It is recommended that you enable this option. This option is available only if you enable 11h support.
Process client IE requests	Select to enable the AP to accept IE requests sent by clients via Probe Request frames and responds by including the requested IE's in the corresponding Probe Response frames. By default this option is disabled. It is recommended that you enable this option.
Energy Save Mode	Select to reduce the number of beacons the AP transmits on a BSSID when no client is associated with the BSSID. This reduces both the power consumption of the AP and the interference created by the AP when no client is associated.
Radio Management (11k) support	Select to enable background scan. Optionally, enable Beacon Report and/or Quiet IE.
Egress Filtering Mode	
Enforce explicitly defined "Out" rules	Traffic is filtered as configured. For more information, see Configuring Egress Filtering Mode on page 362.
Apply "In" rules to "out" direction traffic	The role of the source and destination addresses are reversed. For more information, see Configuring Egress Filtering Mode on page 362.
Client Behavior	
Block MU to MU traffic	Select the Block Mu to MU traffic checkbox if you want to prevent two devices associated with this SSID and registered as users of the controller, to be able to talk to each other. The blocking is enforced at the L2 (device) classification level.
802.1D	

Table 45: Advanced WLAN Service Configuration Page (continued)

Field/Button	Description
802.1D Base Port: xxx	The 802.1D Base Port number in the 802.1D area is the port number by which Extreme Management Center recognizes the SSID. It is read-only.
Remote Service	
Remoteable	Select the checkbox if you want to pair this service with a remote service.
Inter-WLAN Service Roaming	
Permit Inter-WLAN Service Roaming	Select to enable a client on a controller to maintain the session, including the IP address and role assignment, while roaming between VNSs having the same SSID and privacy settings. If not selected, when the client roams among VNSs, the existing session terminates and a new session starts with the client having to associate and authenticate again. The list of VNSs that share the same SSID and privacy settings displays below.
Unauthenticated Behavior	
Discard Unauthenticated Traffic	Select the checkbox to drop all traffic flowing to and from an unauthenticated station.
Default Non-Authenticated Policy	Select the checkbox to apply the default non-authenticated policy to all traffic flowing to and from an unauthenticated station.
Netflow	Click to Enable/Disable Netflow flag. For more information, see Using Netflow/MirrorN on page 370.
Apply	Click to apply changes.
Cancel	Click to close the Advanced dialog without saving changes.

Configuring Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques. The controller provides several privacy mechanisms to protect data over the WLAN.

The following are privacy options:

- **None**
- **Static Wired Equivalent Privacy (WEP)** — Keys for a selected VNS, so that it matches the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 VNSs. For each VNS, only one WEP key can be specified. It is treated as the first key in a list of WEP keys.
- **Dynamic Keys** — The dynamic key WEP mechanism changes the key for each user and each session.
- **Wi-Fi Protected Access (WPA)**
 - version 1 with encryption by temporal key integrity protocol (TKIP)
 - version 2 with encryption by advanced encryption standard with counter-mode/CBC-MAC protocol (AES-CCMP)
- **Wi-Fi Protected Access (WPA) Pre-Shared key (PSK)** — Privacy in PSK mode, using a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK is a security solution that adds

authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.



Note

Regardless of the AP model or WLAN Service type, a maximum of 112 simultaneous clients, per radio, are supported by all of the data protection encryption techniques.

About Wi-Fi Protected Access (WPA V1 and WPA V2)



Note

To achieve the strongest encryption protection for your VNS, it is recommended that you use WPA v.1 or WPA v.2.

WPA v1 and WPA v2 add authentication to WEP encryption and key management. Key features of WPA privacy include:

- Specifies 802.1x with Extensible Authentication Protocol (EAP)
- Requires a RADIUS or other authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

The encryption portion of WPA v1 is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet (unicast key) or after the specified re-key time interval (broadcast key) expires
- An enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise
- A Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, which ensures that the message has not been tampered with.

The encryption portion of WPA v2 is Advanced Encryption Standard (AES). AES includes:

- A 128-bit key length, for the WPA2/802.11i implementation of AES
- Four stages that make up one round. Each round is iterated 10 times.
- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval expires.
- The Counter-Mode/CBC-MAC Protocol (CCMP), a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include:
 - Counter mode (CTR) that achieves data encryption
 - Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity

The following is an overview of the WPA authentication and encryption process:

- 1 The wireless device client associates with Wireless APs.
- 2 Wireless AP blocks the client's network access while the authentication process is carried out (the controller sends the authentication request to the RADIUS authentication server).

- 3 The wireless client provides credentials that are forwarded by the controller to the authentication server.
- 4 If the wireless device client is not authenticated, the wireless client stays blocked from network access.
- 5 If the wireless device client is authenticated, the controller distributes encryption keys to the AP and the wireless client.
- 6 The wireless device client gains network access via the AP, sending and receiving encrypted data. The traffic is controlled with permissions and role applied by the controller.

Wireless 802.11n APs and WPA Authentication



Note

If you configure a WLAN Service to use either WEP or TKIP authentication, any wireless 802.11n AP associated to a VNS using that service will be limited to legacy AP performance rates.

If a VNS is configured to use WPA authentication, any wireless 802.11n AP within that VNS will do the following:

- WPA v.1 — If WPA v.1 is enabled, the wireless AP will advertise only TKIP as an available encryption protocol.
- WPA v.2 — If WPA v.2 is enabled, the wireless AP will do the following:
 - If WPA v.1 is enabled, the wireless AP will advertise TKIP as an available encryption protocol.



Note

If WPA v.2 is enabled, the wireless AP does not support the Auto option.

- If WPA v.1 is disabled, the wireless AP will advertise the encryption cipher AES (Advanced Encryption Standard).



Note

The security encryption for some network cards must not be set to WEP or TKIP to achieve a data rate beyond 54 Mbps.

WPA Key Management Options

Wi-Fi Protected Access (WPA v1 and WPA v2) privacy offers you the following key management options:

- None — The wireless client device performs a complete 802.1x authentication each time it associates or tries to connect to an AP.
- Opportunistic Keying — Opportunistic Keying or opportunistic key caching (OKC) enables the client devices to roam fast and securely from one wireless AP to another in 802.1x authentication setup.

The client devices that run applications such as video streaming and VoIP require rapid reassociation during roaming. OKC helps such client devices by enabling them to rapidly reassociate with the APs. This avoids delays and gaps in transmission and thus helps in secure fast roaming (SFR).

**Note**

The client devices should support OKC to use the OKC feature in the WLAN.

- Pre-authentication — Pre-authentication enables a client device to authenticate simultaneously with multiple APs in 802.1x authentication setup. When the client device roams from one AP to another, it does not have to perform the complete 802.1x authentication to reassociate with the new AP as it is already pre-authenticated with it. This reduces the reassociation time and thus helps in seamless roaming.

**Note**

The client devices should support pre-authentication to use the pre-authentication feature in the WLAN.

- Opportunistic Keying & Pre-auth — Opportunistic Keying and Pre-auth options is meant for environments where device clients supporting either authentication method (OKC or Pre-Auth) may be expected. The method that is used in each case is up to the individual client device.

Configuring WLAN Service Privacy

To configure privacy:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **WLAN Services**. The **WLAN Services** window displays.
- 2 Select the desired service to edit from the left pane. The WLAN Service configuration page is displayed.

- Click the **Privacy** tab, then select the desired privacy method. The WLAN Services Privacy tab displays. [Table 46](#) describes the WLAN services privacy tab fields and buttons.

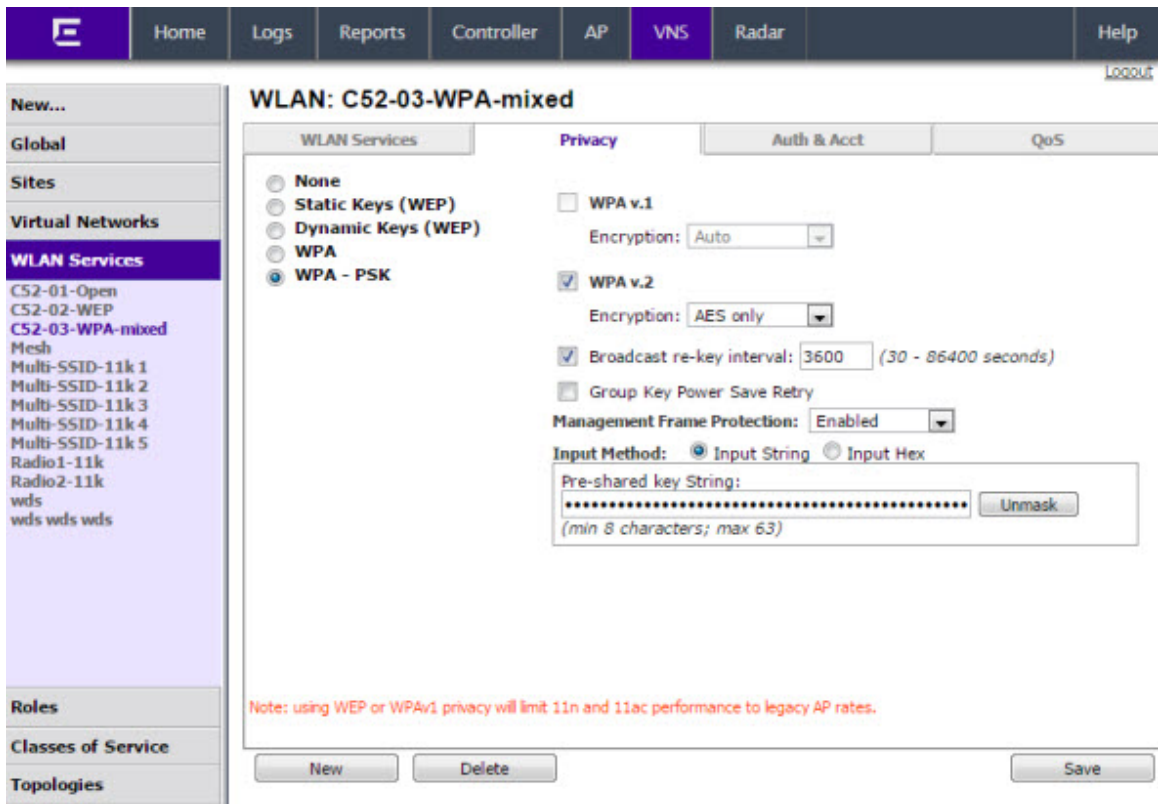


Figure 62: Configuring WLAN Service Privacy

Table 46: WLAN Services Privacy Tab - Fields and Buttons

Field/Button	Description
None	Select to configure a WLAN service with no privacy settings.
Static Keys (WEP)	Select to configure static key (WEP) privacy settings.
WEP Key Index	From the WEP Key Index drop-down list, select the WEP encryption key index. Options are 1 to 4. This field is available only when configuring static keys.
WEP Key Length	From the WEP Key Length drop-down list, click the WEP encryption key length . Options are: 64-bit, 128-bit, and 152-bit. This field is available only when configuring static keys.

Table 46: WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
Input Method	<p>Select one of the following input methods:</p> <ul style="list-style-type: none"> • Input Hex — If you select Input Hex, type the WEP key input in the WEP Key box. The key is generated automatically, based on the input. • Input String — If you select Input String, type the secret WEP key string used for encrypting and decrypting in the Strings box. The WEP Key box is automatically filled by the corresponding Hex code. <p>This field is available only when configuring static keys.</p>
WEP Key	Type the WEP key using the input method chosen above.
Dynamic Keys (WEP)	Select to configure dynamic keys (WEP) privacy settings.
WPA	Select to configure WPA privacy settings.
WPA - PSK	Select to configure dynamic keys (WEP) privacy settings.
WPA v.1	<p>Select the checkbox to enable WPA v.1 encryption, and then select an encryption method:</p> <p>Auto — If you click Auto, the AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.</p> <p>TKIP only — If you click TKIP, the AP advertises TKIP as an available encryption protocol. It will not advertise CCMP.</p> <p>This field is available only when configuring WPA and WPA - PSK privacy settings.</p> <p>Note: TKIP is no longer a supported configuration. Instead you will be directed to configure WPA/WPA2 mixed mode security.</p>

Table 46: WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
WPA v.2	<p>Select the checkbox to enable WPA v.2 encryption, and then select an encryption method:</p> <p>Auto — If you click Auto, the AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.</p> <p>AES only — If you click AES, the AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.</p> <p>This field is available only when configuring WPA and WPA - PSK privacy settings.</p> <p>TKIP — If you click AES, the wireless AP advertises CCMP as an available encryption protocol.</p>
Key Management Options	<p>Click one of the following key management options:</p> <ul style="list-style-type: none"> • None — The mobile units (client devices) perform a complete 802.1x authentication each time they associate or connect to an AP. • Opportunistic Keying — Enables secure fast roaming (SFR) of mobile units. For more information, see Configuring WLAN Service Privacy on page 285. • Pre-authentication — Enables seamless roaming. For more information, see Configuring WLAN Service Privacy on page 285. • Opportunistic Keying & Pre-auth — For more information, see Configuring WLAN Service Privacy on page 285.
Broadcast re-key interval	<p>To enable re-keying after a time interval, select the Broadcast re-key interval box, then type the time interval after which the broadcast encryption key is changed automatically. The default is 3600 seconds. If this checkbox is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions which will reduce the level of security for wireless communications.</p>
Management Frame Protection	<p>Select to enable or disable frame protection for WPA v.2 privacy.</p>
Fast Transition	<p>Click to Enable for 11r enabled APs. This feature only applies to 37xx and 38xx APs.</p>
Input Method	<p>Select one of the following input methods:</p> <ul style="list-style-type: none"> • Input Hex — If you select Input Hex, type the pre-shared key as hex characters. • Input String — If you select Input String, type the pre-shared key as a string of characters.

Table 46: WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
Pre-shared key String	In the Pre-Shared Key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. To proofread your entry before saving the configuration, click Unmask to display the Pre-Shared Key. To mask the key, click Mask
Save	Click to save the configuration.

Configuring Accounting and Authentication

The next step in configuring a WLAN Service is to set up the authentication mechanism. There are various authentication modes available:

- None
- Internal Captive Portal
- External Captive Portal
- GuestPortal
- GuestSplash
- Firewall-Friendly External Captive Portal
- 802.1x authentication (The wireless device user must be authenticated before gaining network access.)



Note

You cannot configure accounting and authentication for a remote WLAN service. The authentication that you configure for the corresponding remoteable WLAN service applies to the remote WLAN service as well.

The first step for any type of authentication is to select RADIUS servers for the following:

- Authentication
- Accounting
- MAC-based authentication

For more information, see [Configuring Basic Captive Portal Settings](#) on page 302

Defining Accounting Methods for a WLAN Service

Accounting tracks the activity of wireless device users. There are two types of accounting available:

- **Controller accounting** — Enables the controller to generate Call Data Records (CDRs), containing usage information about each wireless session. CDR generation is enabled on a per VNS basis. For more information on CDRs, refer to section [Call Detail Records \(CDRs\)](#) on page 610.
- **RADIUS accounting** — Enables the controller to generate an accounting request packet with an accounting start record after successful login by the wireless device user, and an accounting stop record based on session termination. The controller sends the accounting requests to a remote RADIUS server.

Controller accounting creates Call Data Records (CDRs). If RADIUS accounting is enabled, a RADIUS accounting server needs to be specified.

To define accounting methods:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to define accounting methods for. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.
- 4 Click **Enable MAC-based authentication**.

The screenshot shows the configuration page for WLAN Service CNL-422-0-0. The 'Auth & Acct' tab is selected. Under 'Authentication', the mode is set to 'Internal'. The 'Enable MAC-based authentication' checkbox is checked. In the 'RADIUS Servers' section, a table lists the 'Smoke Test RADIUS Server' with 'Auth', 'MAC', and 'Acct' columns checked. A 'Collect Accounting Information of Wireless Controller' checkbox is also checked. The left sidebar shows the 'WLAN Services' menu expanded to 'CNL-422-0-0'. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radars', and 'Help'.

Figure 63: Defining Accounting Methods

- 5 Click the **Configure** button to open the **MAC-Based Authorization** dialog.

Figure 64: MAC-Based Authorization Configuration

Table 47: MAC-Based Authorization Configuration - Fields and Buttons

Field/Button	Description
MAC-based authorization on room	Select method for MAC-based authorization: Never: disables the feature On inter-AP roam: enables MAC-based authorization on roam. On inter-Area roam: enables MAC-based authorization sent to the RADIUS server on area roams.
Automatically Authenticate Authorized Users	Select to automatically authenticate authorized users. When set, a station that passes MAC-based authentication is treated as fully authorized. For example, its authentication state is set to fully authenticated. This can trigger a change to the role applied to the station. If Captive Portal authentication is also configured on the WLAN Service, a station that passes MAC-based authentication will not have to pass Captive Portal authentication as well.
Allow Un-Authorized Users	Select to allow un-authorized users which permits stations that do not pass MAC-based authentication to stay on the network in an un-authorized state. The station can be confined to a “Walled Garden” by its assigned role. If Captive Portal authentication is also configured on the WLAN Service, a station that fails MAC-based authentication can still become authorized by passing Captive Portal authentication. Note: Only select this checkbox if you want your clients to be authorized every time they roam to another AP. If this option is not enabled, and MAC-based authentication is in use, the client is authenticated only at the start of a session.
RADIUS accounting begins after MAC-based authorization completes	Select to delay RADIUS accounting until after MAC-based authorization is complete.
RADIUS Server Timeout Role	Select a Radius Server Timeout Role from the drop-down list.

- 6 To enable Controller accounting, select **Collect Accounting Information of Wireless Controller**.

- 7 To enable RADIUS accounting, from the **RADIUS Servers** drop-down list, click the RADIUS server you want to use for RADIUS accounting, and then click **Use**.

The server name is added to the **Server** table of assigned RADIUS servers. The selected server is no longer available in the RADIUS servers drop-down list.

The RADIUS servers are defined on the **Global Settings** screen. For more information, see [Defining RADIUS Servers and MAC Address Format](#) on page 346.

- 8 In the **Server** table, select the checkbox in the **Acct** column to enable accounting for each applicable RADIUS server.
- 9 In the **Server** table click the RADIUS server, and then click **Configure**. The **RADIUS Parameters** dialog is displayed.

The configured values for the selected server are displayed in the table at the top.

RADIUS Parameters Server: 3222

	Port	Timeout	NAS IP	NAS Identifier	Auth Type
MAC	1812	5	VNS IP	VNS NAME	PAP
Acct	1813	5	VNS IP	VNS NAME	-

NAS IP Address: Use VNS IP address or use:

NAS Identifier: Use VNS name or use:

Auth. type: PAP

Password:

Figure 65: RADIUS Parameters dialog

- 10 For **NAS IP Address**, accept the default of “Use VNS IP address” or de-select the checkbox and type the IP address of a Network Access Server (NAS).
- 11 For **NAS Identifier**, accept the default of “Use VNS name” or type 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.
- 12 For **Auth. type**, select the Protocol using the drop down list. Choices are PAP, CHAP, MS-CHAP, or MS-CHAP2.
- 13 In the **Password** box, type the password that will be passed to RADIUS for wireless MAC authentication.

To proofread your shared secret key, click **Unmask**. The password is displayed.
- 14 Click **OK**.
- 15 To save your changes, click **Save**.

Configuring Authentication for a WLAN Service

- **802.1x Authentication** — If 802.1x authentication mode is configured, the wireless device must successfully complete the user authentication verification prior to being granted network access. This enforcement is performed by both the user's client and the AP. The wireless device's client utility must support 802.1x. The user's EAP packets request for network access along with login identification or a user profile is forwarded by the controller to a RADIUS server.
- **Captive Portal Authentication** — For Captive Portal authentication, the wireless device connects to the network, but can only access the specific network destinations defined in the non-authenticated filter. For more information, see [Policy Rules](#) on page 243. One of these destinations should be a server, either internal or external, which presents a Web login page — the Captive Portal. The wireless device user must input an ID and a password. This request for authentication is sent by the controller to a RADIUS server or other authentication server. Based on the permissions returned from the authentication server, the controller implements role and allows the appropriate network access.

Captive Portal authentication relies on a RADIUS server on the enterprise network. There are three mechanisms by which Captive Portal authentication can be carried out:

- **Internal Captive Portal** — The controller displays the Captive Portal Web page, carries out the authentication, and implements role.
- **External Captive Portal** — After an external server displays the Captive Portal Web page and carries out the authentication, the controller implements role.
- **External Captive Portal with internal authentication** — After an external server displays the Captive Portal Web page, the controller carries out the authentication and implements role.
- **RADIUS servers** — RADIUS servers can perform the following for a WLAN Service:
 - **Authentication** — RADIUS servers are configured to provide authentication.
 - **MAC authentication** — RADIUS servers are configured to provide MAC-based authentication.
 - **Accounting** — RADIUS servers are configured to provide accounting services.

MAC-Based Authentication for a WLAN Service

- **MAC-based authentication** — MAC-based authentication enables network access to be restricted to specific devices by MAC address. The controller queries a RADIUS server for a MAC address when a wireless client attempts to connect to the network.
- MAC-based authentication can be set up on any type of WLAN Service. To set up a RADIUS server for MAC-based authentication, you must set up a user account with UserID=MAC and Password=MAC (or a password defined by the administrator) for each user. Specifying a MAC address format and role depends on which RADIUS server is being used.
- If MAC-based authentication is to be used in conjunction with the 802.1x or Captive Portal authentication, an additional account with a real UserID and Password must also be set up on the RADIUS server.

MAC-based authentication responses may indicate to the controller what VNS a user should be assigned to. Authentication (if enabled) can apply on every roam.

Assigning RADIUS Servers for Authentication

To assign RADIUS servers for authentication:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service.
- 3 Click the **Auth & Acct** tab.

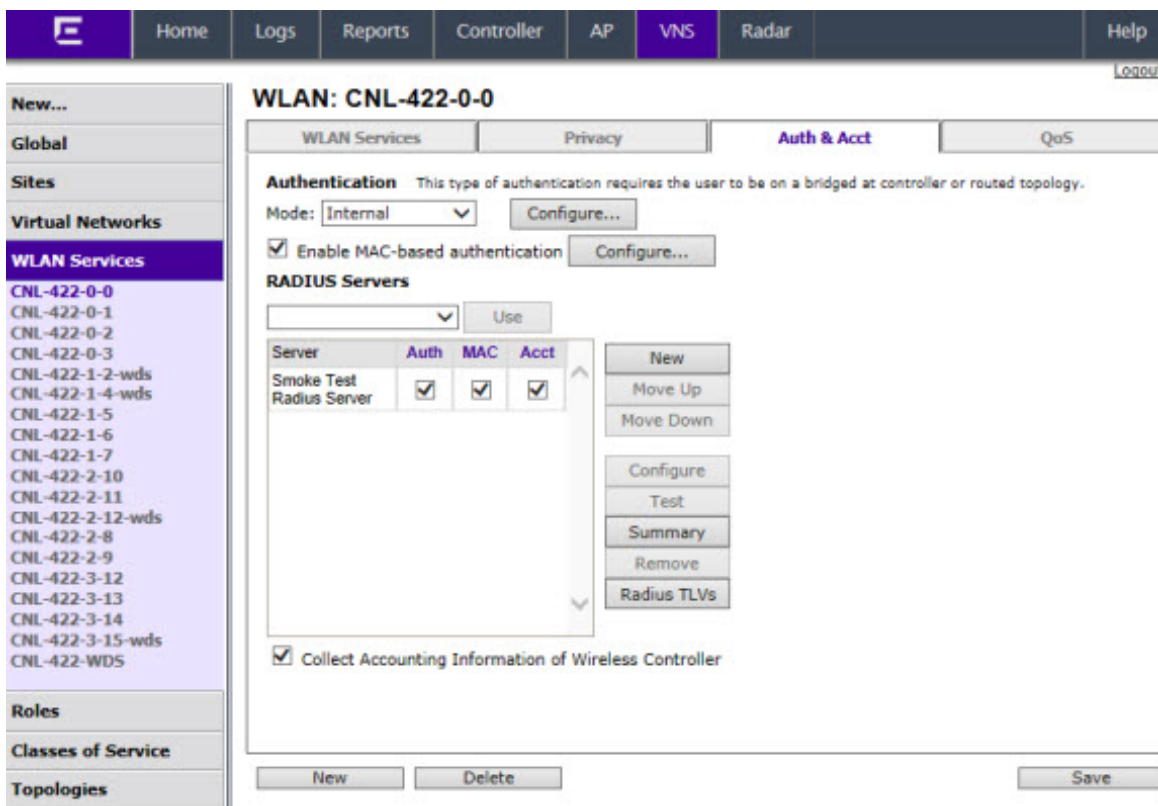


Figure 66: Auth & Acct Tab

Table 48: WLAN Services Auth & Acct Tab - Fields and Buttons

Field/Button	Description
Authentication	
Mode	Select an authentication mode from the drop-down list: <ul style="list-style-type: none"> • Disabled • 802.1x • Internal • External • Firewall Friendly External • Guest Portal • Guest Splash
Configure	Click to configure the selected mode. For more information, see Configuring Accounting and Authentication on page 289.
Enable MAC-based authentication	Select to enable the RADIUS server to perform MAC-based authentication for the VNS with Captive Portal.

Table 48: WLAN Services Auth & Acct Tab - Fields and Buttons (continued)

Field/Button	Description
RADIUS Servers	<p>Select the server you want to assign to the WLAN Service from the drop-down list, then click Use.</p> <p>The server name is added to the Server table of assigned RADIUS servers. The selected server is no longer available in the RADIUS servers drop-down list.</p> <p>The RADIUS servers are defined on the Global Settings screen. For more information, see Defining RADIUS Servers and MAC Address Format on page 346.</p> <p>In the Server table, select the checkboxes in the Auth, MAC, or Acct columns, to enable the authentication or accounting, if applicable.</p>
Collect Accounting Information of Wireless Controller	Select this checkbox to enable Controller accounting.

Note

Both MAC-based Authorization settings work together so that a station can be allowed onto a WLAN Service if it passes MAC-based authentication or Captive Portal authentication. Owners of known stations do not have to enter credentials and owners of unknown stations can get onto the network, if authorized, via Captive Portal.

- Click the **Radius TLVs** button to open the RADIUS Access-Request Message Options dialog.

Figure 67: RADIUS Access Request Message Options

Table 49: RADIUS TLVs Dialog - Fields and Buttons

Field/Button	Description
VSAs	
Vendor-Specific-Attributes in RADIUS Requests	<p>Select the appropriate checkboxes to include the Vendor Specific Attributes (VSAs) in the message to the RADIUS server:</p> <ul style="list-style-type: none"> • Ingress Rate Control • Egress Rate Control • Topology Name • Role Name • VNS Name • AP Name • SSID <p>For more information, see Defining Common RADIUS Settings on page 297.</p>
Optional TLVs	
Chargeable-User-Identity	Select to NOT return a Chargeable-User-Identity attribute for the RADIUS Server.
Treat Access-Accept without Chargeable-User-Identity attribute as Access-Reject	Select to enable feature.
Zone Support	
Replace Called Station ID with Zone name in RADIUS Requests	Select this checkbox to allow the RADIUS client to send the AP Zone as the Called-Station ID instead of the radio MAC address. This feature can be enabled regardless of whether the Site is using centrally located or local RADIUS servers.
Operator Name	Select the name of the user assigned to this RADIUS server from the drop-down list. Once a name is selected, a text box displays to allow text to be entered.

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

Defining the RADIUS Server Priority for RADIUS Redundancy

If more than one server has been defined for any type of authentication, you can define the priority of the servers in the case of failover.

In the event of a failover of the main RADIUS server—if there is no response after the set number of retries—then the other servers in the list will be polled on a round-robin basis until a server responds.

If all defined RADIUS servers fail to respond, a critical message is generated in the logs.

To Define the RADIUS Server Priority for RADIUS Redundancy:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service.
The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.

- 4 In the **Server** table, click the RADIUS server and then click **Move Up** or **Move Down** to arrange the order. The first server in the list is the active one.
- 5 To save your changes, click **Save**.

Configuring Assigned RADIUS Servers

Configuring assigned RADIUS servers for a VNS can include the following:

- [Defining Common RADIUS Settings](#) on page 297
- [Defining RADIUS Settings for Individual RADIUS Servers](#) on page 298
- [Testing RADIUS Server Connections](#) on page 299
- [Viewing the RADIUS Server Configuration Summary](#) on page 300
- [Removing an Assigned RADIUS Server from a WLAN Service](#) on page 301

Defining Common RADIUS Settings

To Define Common RADIUS Settings:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.
- 4 In the **RADIUS Servers** section, click the **Radius TLVs** button and select the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server. For more information, see [Vendor Specific Attributes](#) on page 297.
- 5 To save your changes, click **Save**.

Vendor Specific Attributes

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The ExtremeWireless authentication mechanism provides VSAs for RADIUS and other authentication mechanisms ([Table 50](#)).

Table 50: Vendor Specific Attributes

Attribute Name	ID	Type	Messages	Description
AP-Name	2	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign role based on AP name or location.
AP-Serial	3	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.
AP Ethernet MAC		string	Sent to RADIUS server	The MAC address of the AP used by the ECP to determine client location.
AP Location		string	Sent to RADIUS server	The physical location of the AP. Provided by the network administrator.

Table 50: Vendor Specific Attributes (continued)

Attribute Name	ID	Type	Messages	Description
VNS-Name	4	string	Sent to RADIUS server	The name of the Virtual Network the client has been assigned to. It is used in assigning role and billing options, based on service selection.
SSID	5	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning role and billing options, based on service selection.
BSS-MAC	6	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning role and billing options, based on service selection and location.
Role-Name	7	string	Sent to RADIUS server	The name of the role applied to the station's session.
Topology-Name	8	string	Sent to RADIUS server	The name of the topology applied to the station's session.
Ingress-RC-Name	9	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's outbound traffic.
Egress-RC-Name	10	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's inbound traffic.

The RADIUS message also includes RADIUS attributes Called-Station-Id and Calling-Station-Id to include the MAC address of the wireless device.

**Note**

Siemens-URL-Redirection is supported by MAC-based authentication.

Defining RADIUS Settings for Individual RADIUS Servers

To Define RADIUS Settings for Individual RADIUS Servers:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.

- In the **Server** table, click the RADIUS server you want to define, and then click **Configure**. The **RADIUS Parameters** dialog is displayed.

RADIUS Parameters Server: 3222

	Port	Timeout	NAS IP	NAS Identifier	Auth Type
MAC	1812	5	VNS IP	VNS NAME	PAP
Acct	1813	5	VNS IP	VNS NAME	-

NAS IP Address: Use VNS IP address or use:

NAS identifier: Use VNS name or use:

Auth. type:

Password:

- For **NAS IP Address**, accept the default of “Use VNS IP address” or de-select the checkbox and type the IP address of a Network Access Server (NAS).
- For **NAS Identifier**, accept the default of “Use VNS name” or type 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.
- For **Auth. type**, select the Protocol using the drop down list. Choices are PAP, CHAP, MS-CHAP, or MS-CHAP2.
- In the **Password** box, type the password that will be used to validate the connection between the controller and the RADIUS server.
To proofread your shared secret key, click **Unmask**. The password is displayed.
- Click **OK**.
- To save your changes, click **Save**.

Testing RADIUS Server Connections

To Test RADIUS Server Connections:

- From the top menu, click **VNS**.
- In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- Click the **Auth & Acct** tab.

- 4 In the **Server** table, click the RADIUS server whose connection you want to test, and then click **Test**.

The RADIUS test is a test of connectivity to the RADIUS server, not of full RADIUS functionality. The controller's RADIUS connectivity test initiates an access-request, to which the RADIUS server will respond. If a response is received (either access-reject or access-accept), then the test is deemed to have succeeded. If a response is not received, then the test is deemed to have failed. In either case, the test ends at this point.

If the WLAN Service Authentication mode is Internal or External Captive Portal, or if MAC-Based Authorization is selected, then this test can also test a user account configured on the RADIUS server. In these cases, if proper credentials are filled in for User ID and Password, an access-accept could be returned.

If the WLAN Service Authentication mode is 802.1x, however, an Access-Reject is expected if the RADIUS server is accessible, and the test is considered a success.

Figure 68: Test RADIUS Server

- 5 In the **User ID** box, type the user ID that you know can be authenticated.
- 6 In the **Password** box, type the corresponding password. A password is not required for a AAA VNS.
- 7 Click **Test**. The **Test Result** screen displays.
- 8 Click **Close** after reviewing the test results.
- 9 To save your changes, click **Save**.

Viewing the RADIUS Server Configuration Summary

To View the RADIUS Server Configuration Summary:

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

- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.
- 4 In the **Server** table, click a RADIUS server whose configuration summary you want to view, and then click **Summary**. The **RADIUS Summary** screen displays.

Server	Use For	Priority	Port	# of Retries	Timeout	NAS Identifier	Auth. Type
Smoke Test Radius Server							
	Auth	1	1812	3	5	CNL-422-0-0	PAP
	MAC	1	1812	3	5	CNL-422-0-0	CHAP
	Acct	1	1813	3	5	CNL-422-0-0	N/A

Figure 69: RADIUS Summary

- 5 Click **Close**.
- 6 To save your changes, click **Save**.

Removing an Assigned RADIUS Server from a WLAN Service

To remove an assigned RADIUS Server from a WLAN Service:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane and click the WLAN Service you want to define accounting methods for.
- 3 Click the **Auth & Acct** tab.
- 4 In the **Server** table, click the assigned RADIUS server that you want to remove from the VNS, and then click **Remove**. The RADIUS server is removed from the VNS.
- 5 Click **Save**.

Defining a WLAN Service with No Authentication

You can set up a WLAN Service that will bypass all authentication mechanisms and run the ExtremeWireless Appliance with no authentication of a wireless device user.

A WLAN Service with no authentication can still control network access using policy rules. For more information on how to set up policy rules that allow access only to specified IP addresses and ports, see [Policy Rules](#) on page 243.

To define a WLAN Service with No Authentication:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to configure or click **New**.
- 3 Configure the service as described in [WLAN Services Overview](#) on page 273.
- 4 Click the **Auth & Acct** tab.

- 5 From the **Authentication Mode** drop-down list, select **Disabled**.
- 6 Click **Save**.

Configuring Captive Portal for Internal or External Authentication

Captive Portal allows you to require network users to complete a defined process, such as logging in or accepting a network usage role, before accessing the Internet.

The Captive Portal options are:

- **802.1x** - Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the controller request to a RADIUS server.
- **Internal Captive Portal** — Define the parameters of the internal Captive Portal page displayed by the controller, and the authentication request from the controller to the RADIUS server.
- **External Captive Portal** — Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the appliance request to a RADIUS server.
- **Firewall Friendly External** — Define the parameters of the Firewall Friendly Captive Portal page displayed by an external server. This parameter minimizes the need to open firewall ports and any device on the secure side is allowed to connect to the Internet on port 80, 443.
- **GuestPortal** — Define the parameters for a GuestPortal Captive Portal page. A GuestPortal provides wireless device users with temporary guest network services.
- **Guest Splash** — Define the parameters of the Guest Splash page displayed by the controller. These parameters are similar to those for an internal Captive Portal page, except that the options to configure the labels for user id and password fields are not present since login information is not required when the user is re-directed to the authorization web page. This type of Captive Portal could be used where the user is expected to read and accept some terms and conditions before being granted network access.

Configuring Basic Captive Portal Settings

When configuring captive portal, different settings become available depending on the captive portal option you choose.

To configure the captive portal settings:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.

- 3 Click the **Auth & Acct** tab.

The screenshot shows the 'Auth & Acct' configuration page for WLAN: CNL-422-0-0. The interface includes a navigation menu on the left with categories like Global, Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main configuration area has tabs for WLAN Services, Privacy, Auth & Acct, and QoS. The Auth & Acct tab is active, showing the following configuration options:

- Authentication:** Mode is set to 'Internal'. A note states: 'This type of authentication requires the user to be on a bridged at controller or routed topology.' There is a 'Configure...' button next to the mode dropdown.
- Enable MAC-based authentication:** This checkbox is checked. There is a 'Configure...' button next to it.
- RADIUS Servers:** A dropdown menu is set to 'Use'. Below it is a table of RADIUS Servers:

Server	Auth	MAC	Acct
Smoke Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Radius Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

 To the right of the table are buttons for 'New', 'Move Up', 'Move Down', 'Configure', 'Test', 'Summary', 'Remove', and 'Radius TLVs'.
- Collect Accounting Information of Wireless Controller:** This checkbox is checked.

At the bottom of the configuration area are buttons for 'New', 'Delete', and 'Save'.

Figure 70: Configuring Basic Captive Portal

- 4 In the **Authentication Mode** drop-down list, select a Captive Portal option.
- Disabled
 - 802.1x
 - Internal
 - External
 - Firewall Friendly External
 - Guest Portal



Note

You must configure a Guest Portal before **Guest Portal** appears as a Captive Portal option. Only one WLANS on a VNS can be configured for Guest Portal.

- Guest Splash

5 Click **Configure**.

The Captive Portal configuration page displays. The page display differs depending on the mode that you have selected:

- Internal and Splash modes, see [Configuring Internal Captive Portal and Guest Splash](#) on page 312
- External and 802.1x modes, see [Configuring External and Mode 802.1 Captive Portal](#) on page 304
- Guest Portal mode, see [Configuring Guest Portal](#) on page 313
- Firewall Friendly External Captive Portal mode, see [Configuring Firewall Friendly External Captive Portal](#) on page 306.

Configuring External and Mode 802.1 Captive Portal

The screenshot shows a window titled "HTTP Redirect" with a "Session Control Interface" section. It contains the following fields and options:

- EWC Connection:** A dropdown menu showing "192.168.3.225" and a text box showing "0". Below it, text reads "External authentication server access. Port range: 32768 - 65535".
- Enable https support
- Encryption:** A dropdown menu showing "None".
- Shared Secret:** A text box. Below it, text reads "Shared secret should be between 16 - 64 characters".
- Redirection URL:** A text box. Below it, text reads "Note: token=<integer_val>&dest=<original_target_url> will be APPENDED to the redirection URL".
- Add EWC IP & Port to redirection URL

At the bottom right, there are "Close" and "Cancel" buttons.

Figure 71: Captive Portal Page for External and 802.1x Modes

Table 51: External Captive Portal Page - Fields and Buttons

Field/Button	Description
Session Control Interface	
EWC Connection	In the drop-down list, click the IP address of the external Web server. and then enter the port of the controller. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Enable HTTPS support	Select Enable https support if you want to enable HTTPS support (TLS/SSL) for this external captive portal. This has no impact on the traffic exchanged between users' browsers and the External Captive Portal. When enabled, this option protects the session control traffic between the external captive portal and the controller from being read by a third party. This is particularly useful when a dedicated network management VLAN is unavailable to carry the session control traffic. For more information, see the <i>Integration Guide</i> .

Table 51: External Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Encryption	<p>Select the data encryption to use. Options are:</p> <ul style="list-style-type: none"> • None—no encryption is performed. If the HTTPS option is not enabled, session control messages are sent in plain text over the network. • Legacy—both the ECP and the controller are expected to use simple message encryption based on . Frames are encrypted by XORing session control message payload with a keystream generated from an MD5 hash of a shared key. This is a weak encryption algorithm and is only supported for backward compatibility. If encryption is needed, consider using the option below. • AES—session control messages sent by the controller and ECP are encrypted with the “Advanced Encryption Standard” based on the Rijndael cipher. AES encryption is considerably more secure than legacy encryption. <p>If encryption is enabled then a shared key must be entered.</p> <p>Note: Using the encryption option has one advantage over using the HTTPS option alone. When HTTPS is enabled, the ECP can authenticate the controller’s certificate, but the controller does not ask the client to provide one. Consequently, HTTPS does not prevent unauthorized users from sending messages to the session control interface. Because the encryption option is based on a shared key, the encryption provides a form of authentication. If the controller can decrypt the payload of a session control message, then it has reason to believe the message came from the external captive portal.</p>
Shared Secret	<p>Type the password common to both the controller and the external web server if you want to encrypt the information passed between the controller and the external web server. If encryption is enabled then a shared key must be entered. A shared key is a string that both the controller and the ECP use to encrypt and decrypt session control messages. The shared key must be between 16 and 64 characters long. For better security, use a long key composed of randomly selected characters.</p>
Redirection URL	<p>The Redirection URL field contains the URL to which the controller will redirect all blocked, unauthenticated HTTP traffic on this WLAN Service, or traffic that has been explicitly configured for redirection, depending on your configuration. This should be the URL of the page that will prompt the user to authenticate. If using host name rules, the redirection url can be the configured host name. The redirected browser will issue a “get” to the ECP for this URL. The “Redirection URL”:</p> <ul style="list-style-type: none"> • Can begin with “http://” or “https://”. • Must end with a “?” or “&”. Use “&” if the base URL contains some query strings. <p>Note: The Redirection URL does not support IPv6.</p>

Table 51: External Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Add EWC IP & Port to redirection URL	The Add HWC IP & Port to redirection URL option is useful if the external captive portal serves more than one controller. An ECP must send its session control messages to the controller hosting the controlled session. If an ECP serves more than one controller, then the Add HWC IP & Port to redirection URL option must be used to identify the source of the redirection. The ECP should store the controller address and port with the token and other session details so that it is available throughout the authentication process.
Special	
ToS override for NAC	Allows for ToS marking results in redirection to a captive portal via a NAC server.
Close	Click to save your changes and close this page.
Cancel	Click to discard the configuration

**Note**

You must add a role rule to the non-authenticated filter that allows access to the external Captive Portal site. For more information, see [Policy Rules](#) on page 243.

Related Links

[Configuring Basic Captive Portal Settings](#) on page 302

[Policy Rules](#) on page 243

Configuring Firewall Friendly External Captive Portal

This task describes how to configure a Firewall Friendly External Captive Portal.

- 1 From the **Auth & Account** tab, in the Mode field, select **Firewall Friendly External**.
- 2 Click **Save**.

The **Configure** button is enabled.

- 3 Configure RADIUS servers for authentication. For more information, see [Assigning RADIUS Servers for Authentication](#) on page 293.

- 4 Click **Configure**.

Configure

Redirect to External Captive Portal

Identity:

Shared Secret:
 Shared secret should be between 16 - 255 characters

Redirection URL:
Note: token=<integer_val>&dest=<original_target_url> will be APPENDED to the redirection URL

EWC/AP IP & port
 Replace EWC IP with EWC FQDN:

AP name & serial number

AP Ethernet MAC

AP Location

Associated BSSID

VNS Name

SSID

Station's MAC address

Currently assigned role

Containment VLAN (if any) of assigned role

Timestamp

Signature

Note: When configuring Redirect to External Captive Portal on the AP:

- The IP/Port field is enabled by default and Replace with EWC FQDN is not supported.

Redirect From External Captive Portal

Use HTTPS for User Connections:

Send Successful Login To: ▼

*

Figure 72: Configuring Firewall Friendly External Captive Portal

ExtremeWireless offers a scalable external captive portal (ECP) solution on the AP that can be managed locally or through a Cloud solution, in addition to the controller based ECP. The following table illustrates the WLAN redirection configuration options for the AP and the controller. Each setting is identified as mandatory or optional for redirection on the AP or on the controller. For more information about configuring ECP on an AP, see [Configuring a Captive Portal on an AP](#) on page 196

Table 52: Firewall Friendly External Captive Portal

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Redirect to External Captive Portal			
Identity	Type the name common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.	Mandatory Required for signing the redirected URL. If you do not configure the Identity, the redirector on the AP drops the traffic.	Optional
Shared Secret	Type the password common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.	Mandatory Required for signing the redirected URL. If you do not configure the Shared Secret, the redirector on the AP drops the traffic.	Optional
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication. Note: Ensure the request does not exceed the browser character limit. Older browsers limit requests to 255 characters. Newer browsers allow up to 2048 characters. The Redirection URL does not support IPv6.	Mandatory	Mandatory
EWC IP and Port	IP address and Port number	Mandatory By default, this option is enabled. The IP address and port of the AP are always URL parameters. A deployment will have multiple APs. The IP address and port communicate to the External Captive Portal through the client, identifying which AP is redirecting the client.	Optional This option is not required when the deployment includes only one controller. However, we recommend enabling this option when the deployment includes multiple controllers.

Table 52: Firewall Friendly External Captive Portal (continued)

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Replace EWC IP with EWC FQDN	Use controller's Fully-Qualified Domain Name instead of IP address.	Not supported	Optional You can enable this setting if the deployment uses a single controller.
AP Name and Serial Number	Name and Serial Number of AP	N/A AP has this information locally.	Optional
AP Ethernet MAC	MAC address of the AP	N/A AP has this information locally.	Optional
AP Location	Text string used to describe physical AP location.	Optional	Optional
Associated BSSID	Associated BSSID of AP	N/A AP has this information locally.	Optional
VNS Name	Virtualized Network Service Name	Optional For non-site deployments, the VNS Name is not available on the AP. Therefore, it must be included in the mobile user associated response or as part of the mobile user update requirement from the controller.	Optional
SSID	Service Set Identifier	N/A AP has this information locally.	Optional
Station MAC Address	Media Access Control Address	N/A AP has this information locally.	Optional
Currently Assigned Role		Optional For non-site deployments, the Assigned Role is not available on the AP. Therefore, it must be included in the mobile user associated response or as part of the mobile user update requirement from the controller.	Optional

Table 52: Firewall Friendly External Captive Portal (continued)

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Containment VLAN of Assigned Role		Optional For non-site deployments, the Assigned Role is not available on the AP. Therefore, it must be included in the mobile user associated response or as part of the mobile user update requirement from the controller.	Optional
Timestamp	Timestamp (in UTC)	Mandatory The timestamp (in UTC) is always included, because it prevents replay attacks of a recorded redirected URL. The AP must have access to UTC time, which is provided by the controller.	Optional
Signature		Optional Signature is included when full authentication is employed. If configuring a RADIUS authentication server, clear the Signature checkbox. The Signature option is the flag that indicates how authentication is achieved.	Optional
Redirect From External Captive Portal			
Use HTTPS for Users Connections	Select this option to use HTTPS instead of HTTP. The default state will be set for HTTPS. This applies to both new WLANS and WLANS that existed prior to upgrading to V9.15 and later.	Optional The AP presents a self-signed certificate that triggers a warning page in most browsers. The AP does <i>not</i> support installing signed certificates from a trusted certificate authority.	Optional

Table 52: Firewall Friendly External Captive Portal (continued)

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Send Successful Login to:	Select the IP address of the external Web server, and then enter the port of the controller.	Mandatory The session management page can contain a link to the original URL that was served when it was redirected. The session management page includes a button to terminate the user's session. The only way the client can come directly to this page is by replaying the redirection URL from the External Captive Portal within the grace period measured by the timestamp.	Optional The session management page <i>does</i> include a button to terminate the user's session.
View Sample	Displays an example format of the redirection URL that the controller/AP expects to receive (indirectly) from the ECP. If the WLAN Service is part of a VNS or has a default topology, then the server portion of the URL contains the IP address of the controller/AP. The query string is populated with realistic but fictional data. This information is provided to assist in developing the ECP program.		

Configuring Internal Captive Portal and Guest Splash

Configure [?] [X]

Message Configuration

Configure

Communication Options

Use HTTPS for User Connections:

Replace Gateway IP with FQDN:

Send Successful Login To: original destination

*

Manual Settings Use Zip File

Page width is 790 pixels. Extra contents will be cropped out. Please keep them in reasonable heights.

Launch Captive Portal Editor

*Note: Only supported for VNSs where the topology doesn't change.
Certificates can be added on the Topologies page under the Certificates tab.

Close Cancel

Figure 73: Captive Portal Page Configuration Page for Internal and Guest Splash Modes

Table 53: Captive Portal Page Configuration Page for Internal and Guest Splash Modes - Fields and Buttons

Field/Button	Description
Message Configuration	
Configure	Click to configure error messages that may display on the internal captive portal page. The Message Configuration page displays. See (Configuring Error Messages on page 316).
Communication Options	
Use HTTPS for Users Connections	Select this option to use HTTPS instead of HTTP. The default state will be set for HTTPS. This applies to both new WLANS and WLANS that existed prior to upgrading to V9.01 and later.
Replace Gateway IP with FDQN	Type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.
Send Successful Login To:	
Manual Settings	Select this option if you want to manually define the elements on the Captive Portal page. When you select this option, you enable the Launch Captive Portal Editor button.

Table 53: Captive Portal Page Configuration Page for Internal and Guest Splash Modes - Fields and Buttons (continued)

Field/Button	Description
Use Zip File	Select this option to upload a zip file that contains custom Captive Portal content. The zip file you upload must have a flat structure — it cannot contain any sub-directories. The contents of the zip must adhere to the following file formats: <ul style="list-style-type: none"> Content to be used in the captive portal login page must be in a file named login.htm Content to be used in the captive portal index page must be in a file named index.htm. The number of graphics and the size of the graphics is unlimited, and can be either .gif, .jpg, or .png.
Upload Zip File	Click the Browse button and navigate to the zip file to use for setting up the captive portal.
View Sample Login Page	Click to view the sample login page for this captive portal.
View Sample Index Page	Click to view the sample index page for this captive portal.
Download	Click to download the specified zip file. The File Download page displays.
Launch Captive Portal Editor	Click to launch the Captive Portal Editor. Using the Captive Portal Editor, you can configure the elements on the captive portal page. This button becomes available when you select the Manual Setting radio button.
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Configuring Guest Portal**Note**

You must configure a Guest Portal before **Guest Portal** appears as a Captive Portal option. Only one WLANS on a VNS can be configured for Guest Portal.

Configure
?
✕

GuestPortal

Manage Guest Users
Configure Ticket Page
Configure Password Generator

Account Lifetime: days (0 = no limit)

GuestPortal Manager Can Set Account Lifetime:

Maximum Session Lifetime: hours (0 = no limit)

User ID Prefix:

Maximum Concurrent Session:

Message Configuration

Communication Options

Use HTTPS for User Connections:

Replace Gateway IP with FQDN:

Send Successful Login To:

*

Manual Settings Use Zip File

The page width is 790 pixels. Extra content will be cropped out. Please make sure that the height is also reasonable.

*Note: Only supported for VNSs where the topology doesn't change.
Certificates can be added on the Topologies page under the Certificates tab.

Figure 74: Captive Portal Page for Guest Portal Mode

Table 54: Configure Internal Captive Portal Page - Fields and Buttons

Field/Button	Description
Guest Portal - this section becomes available only when configuring a Guest Portal.	
Manage Guest Users	Click to add and configure guest user accounts. The Manage Guest Users page displays. For information about adding and managing guest users, see Working with GuestPortal Administration on page 635.
Configure Ticket Page	Click to configure the guest portal ticket. The Configure ticket page displays. For information about how to configure and activate guest portal ticket pages, see Working with GuestPortal Administration on page 635.

Table 54: Configure Internal Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Configure Password Generator	Click to configure the guest password. The Configure Password Generator page displays. For information about how to configure and activate guest passwords, see Configuring Guest Password Patterns on page 646
Account Lifetime	Type the account lifetime, in days, for the guest account. A value of 0 specifies no limit to the account lifetime.
Guest Admin Can Set Account Lifetime	Select to enable the guest administrator to set the amount of time for which this account will be active.
Maximum Session Lifetime	Type the maximum session lifetime, in hours, for the guest account. The default 0 value does not limit a session lifetime. The session lifetime is the allowed cumulative total in hours spent on the network during the account lifetime.
User ID Prefix	Type a prefix that will be added to all guest account user IDs. The default is Guest.
Minimum Password Length	Type a minimum password length that will be applied to all guest accounts.
Message Configuration	
Configure	Click to configure error messages that may display on the internal captive portal page. The Message Configuration page displays. See (Configuring Error Messages on page 316).
Communication Options	
Use HTTPS for Users Connections	Select this option to use HTTPS instead of HTTP. The default state will be set for HTTPS. This applies to both new WLANS and WLANS that existed prior to upgrading to V9.01 and later.
Replace Gateway IP with FQDN	Type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.
Send Successful Login To:	
Manual Settings	Select this option if you want to manually define the elements on the Captive Portal page. When you select this option, you enable the Launch Captive Portal Editor button.
Use Zip File	Select this option to upload a zip file that contains custom Captive Portal content. The zip file you upload must have a flat structure — it cannot contain any sub-directories. The contents of the zip must adhere to the following file formats: <ul style="list-style-type: none"> • Content to be used in the captive portal login page must be in a file named login.htm • Content to be used in the captive portal index page must be in a file named index.htm. • The number of graphics and the size of the graphics is unlimited, and can be either .gif, .jpg, or .png.
Upload Zip File	Click the Browse button and navigate to the zip file to use for setting up the captive portal.
View Sample Login Page	Click to view the sample login page for this captive portal.

Table 54: Configure Internal Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
View Sample Index Page	Click to view the sample index page for this captive portal.
Download	Click to download the specified zip file. The File Download page displays.
Launch Captive Portal Editor	Click to launch the Captive Portal Editor. Using the Captive Portal Editor, you can configure the elements on the captive portal page. This button becomes available when you select the Manual Setting radio button.
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Configuring Error Messages

You can configure informational and error messages that a user may encounter when trying to access a captive portal.

To configure error and informational messages:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.
- 4 In the **Authentication Mode** drop-down list, select a Captive Portal option.
- 5 Click **Configure**. The Captive Portal Configuration page displays.

- 6 In the Message Configuration section, click the **Configure** button. The **Message Configuration** page displays.



For more information, see [Table 55](#) on page 317

Understanding the Message Configuration Page

Table 55: Message Configuration Page - Fields and Buttons

Field/Button	Description
Invalid	Enter a message indicating that the user entered an invalid username or password combination.
Success	Enter a message to indicate when a user successfully logs in.
Access Fail	Enter an error message that indicates the a user login was unsuccessful.
Fail	Enter a message indicating an internal error.
Timeout	Enter an error message indicating that the user authentication timed out.
RADIUS shared secret security key fail	Enter an error message indicating that RADIUS shared secret failed.
RADIUS internal error	Enter an error message indicating an internal RADIUS client error
Max RADIUS login fail	Enter a message that indicates that the maximum number of simultaneous captive portal logins have been reached.
Invalid Login parameters	Enter a message indicating that the user entered an invalid username or password combination.
General failure	Enter a message indicating that a general failure has occurred.

Table 55: Message Configuration Page - Fields and Buttons (continued)

Field/Button	Description
Invalid third party parameters	Enter an error message indicating that one or more parameters passed from the external captive portal server to the controller is either invalid or missing.
Authentication in progress fail	Enter a message indicating that the user credentials were not authenticated.
Topology Change	Enter an error message indicating that the topology failed.
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Using the Captive Portal Editor

The Captive Portal Editor enables you to configure the look and feel of a captive portal page.

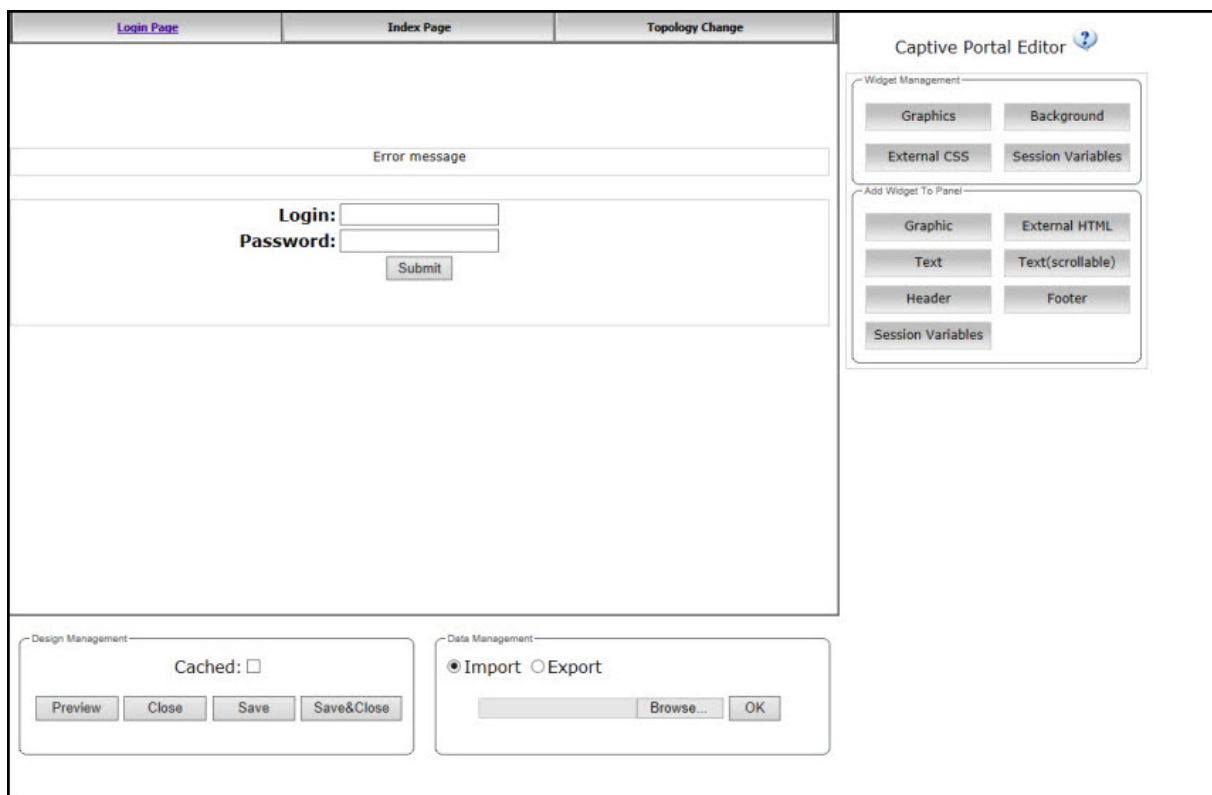
To configure the editor:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand **WLAN Services**, then select the WLAN Service. The **WLAN Services** configuration page displays.
- 3 Click the **Auth & Acct** tab. The **Auth & Accounting** page displays.
- 4 In the **Authentication Mode** drop-down list, select a Captive Portal option.
- 5 Click **Configure**. The **Captive Portal Configuration** page displays.
- 6 In the Communications Options section, select **Manual Settings** and then click **Launch Captive Portal Editor**. For more information, see [Table 56](#) on page 320.



Note

The Captive Portal Editor page supports only one administrator editing a captive portal page at one time.




Caution

In order for Captive Portal authentication to be successful, all the URLs referenced in the Captive Portal setup must also be specifically identified and allowed in the non-authenticated filter. For more information, see [Policy Rules](#) on page 243.



Caution

If you use logos or graphics, ensure that the graphics or logos are appropriately sized. Large graphics or logos may force the login section out of view.

Understanding the Captive Portal Editor

Table 56: Captive Portal Editor - Fields and Buttons

Field/Button	Description
Login Page tab	<p>Click to view and configure the elements that will display on the Captive Portal login page. By default, widgets for a Login username and Password, as well as an Accept button are configured by default. You can accept or change these widgets using the Captive Portal Editor widget management tools in the right-hand panel. Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can:</p> <ul style="list-style-type: none"> • configure the background colors and forms • add graphics • add an external cascading style sheet (.css) • VSA attributes
Index Page Tab	<p>Click to view and configure the elements that will display on the Captive Portal Index page. Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can:</p> <ul style="list-style-type: none"> • configure the background colors and forms • add graphics • add a Logoff button. The Logoff button launches a pop-up logoff page, allowing users to control their logoff. • add a Status Check button The Status check button launches a pop-up window, which allows users to monitor session statistics such as system usage and time left in a session. • add an external cascading style sheet (.css)
Topology Change Tab	<p>Click to view and configure the elements that will display on the Captive Portal Topology change page. By default, a login confirmation and informational message, as well as a Close button, are preconfigured. You can accept or change these elements using the Captive Portal Editor widget management tools in the right-hand panel. Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can:</p> <ul style="list-style-type: none"> • configure the background colors and forms • add graphics • add an external cascading style sheet (.css)
Design Management	
Cached	Select to cache most of the widgets from the design to rescue the amount of time it takes a captive portal page to load.
Preview	Select to view the way the configured widgets will display to a user.
Close	Select to close this page without saving the configuration.
Save	Select to save the configuration changes.
Save&Close	Select to save the configuration changes and close this window.
Data Management	
Import	Select and click Browse to navigate to the directory and filename of the a configuration that you want to import. Click OK to import the configuration.

Table 56: Captive Portal Editor - Fields and Buttons (continued)

Field/Button	Description
Export	Select to save this configuration and enter the name of the file you want to save it in. Click the Browse button to navigate to a directory where you want to store the configuration file. Click OK. to save the configuration.
Widget Management	Use the fields in this section to configure the widgets.
Graphics	Click to locate and upload a graphic. The graphic becomes available in the Show Images section of the Property Editor.
Background	Click to configure the background color of the page
External CSS	Click to identify a cascading style sheet (.css) that will determine the page format.
Session Variables	<p>Click to configure the following VSA attributes:</p> <ul style="list-style-type: none"> • AP Serial • AP Name • VNS Name • SSID • MAC Address <p>The selections influence what URL is returned in either section. For example, wireless users can be identified by which AP or which VNS they are associated with, and can be presented with a Captive Portal Web page that is customized for those identifiers.</p>
Add Widget to Panel	Use the fields in this section to add the configured widgets to the page.
Graphic	Select to add a graphic to the page. Use the Property Editor select a preconfigured graphic, and to determine the size and location of the graphic.
Text	Select to add text to the page. Use the Property Editor to type and format the text, and to determine the location of the text and the conditions under which it displays.
Header	Select to add a Header attribute to the panel. Use the Property Editor to determine the size and position of the Header attribute, the conditions under which it displays, and identify the link and type of Header attribute to include.
Session Variables	Use the Property Editor to determine the size and position of the Header attribute and the conditions under which it displays, select a Display Option, and select a type of VSA.
External HTML	Select to add an external HTML link to the page. Use the Property Editor select a preconfigured graphic, and to determine the size and location of the graphic
Text (Scrollable)	Select to add scrollable text to the page. Use the Property Editor to type and format the text, and to determine the location of the text and the conditions under which it displays.
Footer	Select to add a Footer attribute to the panel. Use the Property Editor to determine the size and position of the Footer attribute, the conditions under which it displays, and identify the link and type of Footer attribute to include.

Defining Priority Level and Service Class

Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks are enabling the integration of internet telephony technology on wireless networks. Various issues including Quality-of-Service (QoS), call control, network capacity, and network architecture are factors in VoIP over 802.11 WLANs.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called isochronous data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn to avoid data collisions. Regular traffic on a wireless network is an asynchronous process in which data streams are broken up by random intervals.

To reconcile the needs of isochronous data, mechanisms are added to the network that give voice data traffic or another traffic type priority over all other traffic, and allow for continuous transmission of data.

To provide better network traffic flow, the controller provides advanced Quality of Service (QoS) management. These management techniques include:

- WMM (Wi-Fi Multimedia) — Enabled on individual WLAN Services, is a standard that provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS.
- IP ToS (Type of Service) or DSCP (Diffserv Codepoint) — The ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality 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.

Defining the Service Class

Service class is determined by the combination of the following operations:

- The class of treatment given to a packet. For example, queuing or per hop behavior (PHB).
- The packet marking of the output packets (user traffic and/or transport).

Table 57: Service Classes

Service class name (number)	Priority level
Network Control (7)	7 (highest priority)
Premium (Voice) (6)	6
Platinum (video) (5)	5
Gold (4)	4
Silver (3)	3
Bronze (2)	2
Best Effort (1)	1
Background (0)	0 (lowest priority)

The service class is equivalent to the 802.1D UP (user priority).

Table 58: Relationship Between Service Class and 802.1D UP

SC name	SC Value	802.1d UP	AC	Queue
Network Control	7	7	VO	VO or TVO
Premium (voice)	6	6	VO	VO or TVO
Platinum (video)	5	5	VI	VI
Gold	4	4	VI	VI
Silver	3	3	BE	BE
Bronze	2	0	BE	BE
Best Effort	1	2	BK	BK
Background	0	1	BK	BK

Configuring the Priority Override

Priority override allows you to define and force the traffic to a desired priority level. Priority override can be used with any combination, as displayed in [Table 58](#) on page 323. You can configure the service class and the DSCP values.

When **Priority Override** is enabled, the configured service class overrides the queue selection in the inbound and outbound directions, the 802.1P UP for the VLAN tagged Ethernet packets, and the UP for the wireless QoS packets (WMM or 802.11e) according to the mapping in [Table 57](#) on page 322. If **Priority Override** is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

Configuring QoS Modes

You can enable the following QoS modes for a WLAN Service:

- **WMM** — If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.
- **802.11e** — If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the inbound traffic.
- **Turbo Voice** — If any of the above QoS modes are enabled, the Turbo Voice mode is available. If enabled, all the out traffic that is classified to the Voice (VO) AC and belongs to that VNS is transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. The TVO queue is tailored in terms of contention parameters and number of retries to maximize voice quality and voice capacity.
- **U-APSD**— Unscheduled Automatic Power Save Delivery feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.

The APs are capable of supporting 5 queues. The queues are implemented per radio. For example, 5 queues per radio. The queues are:

Table 59: Queues

Queue Name	Purpose
AC_VO	Voice
AC_VI	Video
AC_BK	Background
AC_BE	Best Effort
AC_TVO	Turbo Voice

The controller supports the definition of 8 levels of user priority (UP). These priority levels are mapped at the AP to the best appropriate access class. Of the 8 levels of user priority, 6 are considered low priority levels and 2 are considered high priority levels.

WMM clients have the same 4 AC queues. WMM clients will classify the traffic and use these queues when they are associated with a WMM-enabled AP. WMM clients will behave like non-WMM clients—map all traffic to the Best Effort (BE) queue—when not associated with WMM-enabled AP.

The prioritization of the traffic on the downstream (for example, from wired to wireless) and on the upstream (for example, from wireless to wired) is dictated by the configuration of the WLAN Service and the QoS tagging within the packets, as set by the wireless devices and the host devices on the wired network.

Both Layer 3 tagging (DSCP) and Layer 2 (802.1d) tagging are supported, and the mapping conforms with the WMM specification. If both L2 and L3 priority tags are available, then both are taken into account and the chosen AC is the highest resulting from L2. If only one of the priority tags is present, it is used to select the queue. If none is present, the default queue AC_BE is chosen.

Note



If the wireless packets to be transmitted must include the L2 priority (send to a WMM client from a WMM-enabled AP), the outbound L2 priority is copied from the inbound L2 priority if available, or it is inferred from the L3 priority using the above table if the L2 inbound priority is missing.

Table 60: Traffic Prioritization

VNS type	Packet Source	Packet type	L2	L3
Tunneled	Wired	Untagged	No	Yes
Branch	Wired	VLAN tagged	Yes	Yes
Branch	Wired	Untagged	No	Yes
Branch or Tunneled	Wireless	WMM	Yes	Yes
Branch or Tunneled	Wireless	non-WMM	No	Yes

To configure QoS Role:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service.

3 Click the **QoS** tab.

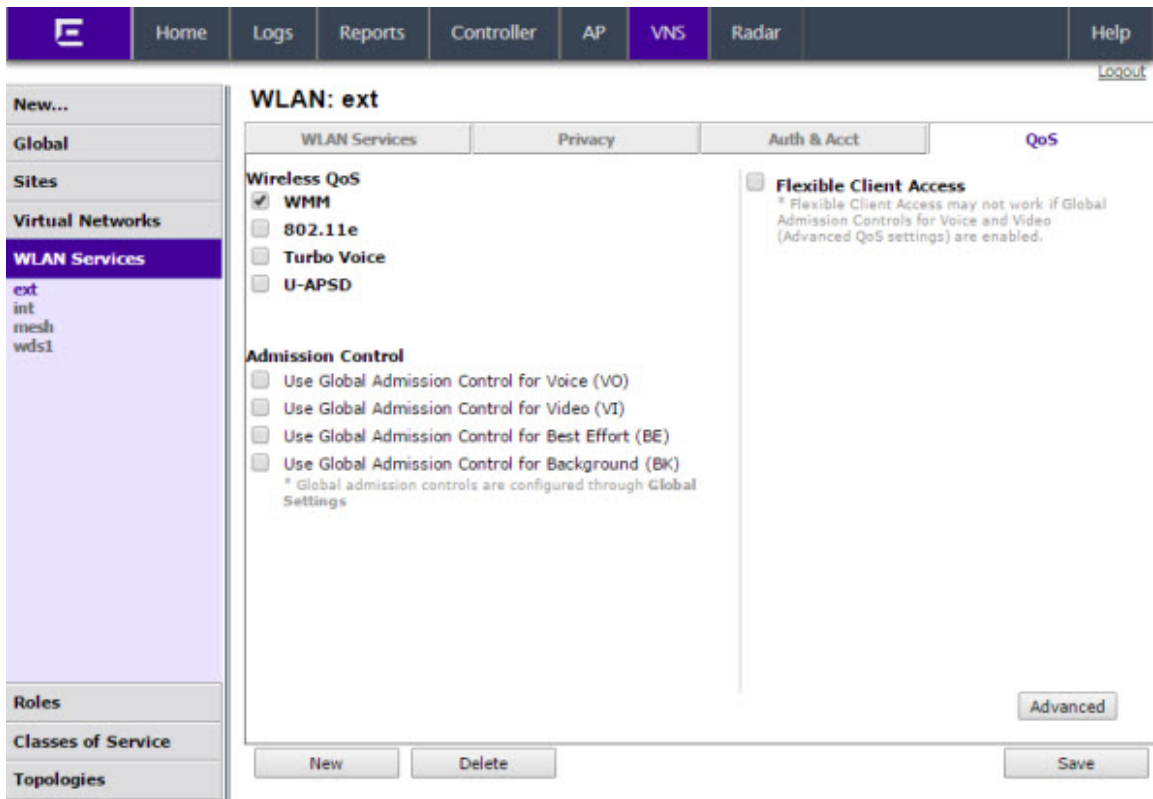


Figure 75: Configuring QoS

Table 61: WLAN Services QoS Tab - Fields and Buttons

Field/Button	Description
Wireless QoS	<p>From the Wireless QoS list, do the following:</p> <p>WMM — Select to enable the AP to accept WMM client associations, and classify and prioritize the outbound traffic for all WMM clients. Note that WMM clients will also classify and prioritize the inbound traffic. WMM is part of the 802.11e standard for QoS. If selected, the Turbo Voice and Enable U-APSD options are displayed.</p> <p>802.11e — Select to enable the AP to accept WMM client associations, and classify and prioritize the outbound traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the inbound traffic. If selected, the Turbo Voice and the Enable U-APSD options are displayed:</p> <p>Turbo Voice — Select to enable all out traffic that is classified to the Voice (VO) AC and belongs to that VNS to be transmitted by the AP via a queue called Turbo Voice (TVQ) instead of the normal Voice (VO) queue. When Turbo Voice is enabled together with WMM or 802.11e, the WMM and/or 802.11e clients in that VNS are instructed by the AP to transmit all traffic classified to VO AC with special contention parameters tailored to maximize voice performance and capacity.</p> <p>Enable U-APSD — Select to enable the Unscheduled Automatic Power Save Delivery (U-APSD) feature. This feature can be used by mobile devices to efficiently sustain one or more real-time streams while being in power-save mode. This feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.</p>
Admission Control	<p>From the Admission Control list, do the following:</p> <p>Use Global Admission Control for Voice (VO) - Select to enable admission control for Voice. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands. For more information, see VNS Global Settings on page 345.</p> <p>Use Global Admission Control for Video (VI) - This feature is only available if admission control is enabled for Voice. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands. Select to provide distinct thresholds for VI (video). For more information, see VNS Global Settings on page 345.</p> <p>Use Global Admission Control for Best Effort (BE) - If the client does not support admission control for the access category that requires admission control, the traffic category will be downgraded to lower access category that does not have Mandatory Admission control. For example, if admission control is required for video, and client does not support admission control for video, traffic will be downgraded to Best Effort (BE).</p>

Table 61: WLAN Services QoS Tab - Fields and Buttons (continued)

Field/Button	Description
	<p>For more information, see VNS Global Settings on page 345.</p> <p>Use Global Admission Control for Background (BK)- This feature is only available if admission control is enabled for Background. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands. For more information, see VNS Global Settings on page 345.</p>
Flexible Client Access	<p>Select the checkbox to enable flexible client access. Flexible client access levels are set as part of the VNS global settings.</p> <p>Note: TSPEC must be disabled when using Flexible Client Access.</p>
Advanced button	
Priority Processing	
Priority Override	<p>Select this checkbox to force DSCP and a service class.</p> <p>Note: When Priority Override is enabled, the configured service class forces queue selection in the outbound direction, the 802.1P user priority for the VLAN tagged Ethernet packets and the user priority for the wireless QoS packets (WMM or 802.11e), according to the mapping between service class and user priority. If Priority Override is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.</p>
DSCP	<p>From the drop-down list, click the DSCP value used to tag the IP header of the encapsulated packets. For more information, see Defining the DSCP and Service Classifications on page 328.</p>
Service Class	<p>Select one of the following service classes:</p> <ul style="list-style-type: none"> • Network control (7) — The highest priority level. • Premium (Voice) (6) • Platinum (5) • Gold (4) • Silver (3) • Bronze (2) • Best Effort (1) • Background (0) — The lowest priority level <p>Note: If you want to assign a service class to each DSCP marking, clear the Priority Override checkbox and define the DSCP service class priorities in the DSCP classification table.</p>

Table 61: WLAN Services QoS Tab - Fields and Buttons (continued)

Field/Button	Description
Advanced Wireless QoS options (Options are only displayed if the WMM or 802.11e checkboxes are selected)	
UL Policer Action	<p>If Use Global Admission Control for Voice (VO) or Use Global Admission Control for Video (VI) is enabled, click the action you want the AP to take when TSPEC violations occurring on the inbound direction are discovered:</p> <p>Do nothing — Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.</p> <p>Send DELTS to Client — Click to end TSPEC violations when it they are discovered. This action deletes the TSPEC.</p>
DL Policer Action	<p>If Use Global Admission Control for Voice (VO) or Use Global Admission Control for Video (VI) is enabled, click the action you want the AP to take when TSPEC violations occurring on the outbound direction are discovered:</p> <p>Do nothing — Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.</p> <p>Downgrade — Click to force the transmission's data packets to be downgraded to the next priority when a TSPEC violation is discovered.</p> <p>Drop — Click to force the transmission's data packets to be dropped when a TSPEC violation is discovered.</p>

Defining the DSCP and Service Classifications

To define the DSCP and Service Class classifications:

All 64 DSCP code-points are supported. The IETF defined codes are listed by name and code. Undefined codes are listed by code. The following is the default DSCP service class classification (where SC is Service Class and UP is User Priority):

Table 62: DSCP Code-Points

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS0/DE	2/0	AF11	2/0	AF33	4/4
CS1	0/1	AF12	2/0	AF41	5/5
CS2	1/2	AF13	2/0	AF42	5/5
CS3	3/3	AF21	3/3	AF43	5/5
CS4	4/4	AF22	3/3	EF	6/6
CS5	5/5	AF23	3/3	Others	0/1

Table 62: DSCP Code-Points (continued)

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS6	6/6	AF31	4/4		
CS7	7/7	AF32	4/4		

Configuring Hotspots

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

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

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

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

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

To Configure a New Hotspot

Configure hotspots under the WLAN Services workbench.

To configure a hotspot:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **WLAN Services**. The **WLAN Services** window displays.
- 2 Click **New** to configure a new WLAN service.
- 3 Provide the service Name, Service Type, and SSID.

- 4 Select the **Hotspot** option. Valid values are:
- **Disabled.** Hotspot functionality is not enabled.
 - **Enabled.** Hotspots are enabled for this WLAN and the **Hotspot** tab appears on the WLAN page.

Privacy is set by default to WPA and Mandatory Frame Protection (MFP) is enable.

The authentication method is set to AAA with External Radius Server;. You can configure MBA, if required .

- **OSU.** Allows the definition of Online Sign Up or OSEN WLAN.



Note

Configure the policy and topology assigned to the OSU WLAN to allow access *only* to the OSU server. No access to the internet.



Note

Once you have defined a WLAN service with a hotspot, you cannot disable the hotspot. You can only delete the WLAN service and recreate it.

- 5 Select the **Hotspot** tab.

Figure 76: Hotspot Configuration

Table 63: WLAN Services Hotspot Tab - Fields and Buttons

Field/Button	Description
HESSID	<p>One SSID can be used across multiple WLANs (BSS), so the HESSID helps a client identify when the BSSID belongs to a homogenous BSS with identical configuration. Beacon with same {HESSID, SSID} pair belong to same WLAN. The {HESSID, SSID} pair must be unique for each WLAN.</p> <p>By default, the HESSID is set to the MAC address of the controller Ethernet port. Hotspots can have the same HESSID as long as the SSID is unique. If opting to configure the HESSID manually, we recommend using an AP BSSID as the HESSID.</p> <p>Note: In a mobility domain, manually configure the HESSID to a unique value, differentiating it from the value used in the controller's WLAN.</p>
Access Network	<p>Identifies the type of network. Valid values are:</p> <ul style="list-style-type: none"> • Private network. An enterprise network with user accounts. • Private network with guest access. An enterprise network providing guest access. • Chargeable public network. (Default) Open to anyone but access requires payment. • Free public network. Open network, free of charge but may still require acceptance of terms of use (and may involve OSU servers with captive portal).
DGAF Disabled	<p>Downstream Group-Address Forwarding Disabled. By default this option is checked. This option is checked when the AP is not forwarding downstream group-addressed frames.</p>

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

Domain. FQDN specified by the user. Default value is empty string.

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

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

- 1 Select a description of the venue group in the first field.
- 2 Select a value from the second field.



Note

The second field is not populated with values until after you select a value from the first field.

Default value is **Unspecified**.

- 7 You can configure up to four languages for each venue. Click the plus sign.

Language	Operator Name	Venue Name
<input checked="" type="checkbox"/> English	John Doe	Capital City Civic Center

Figure 77: Hotspot Identification Tab

A configuration dialog displays.

Figure 78: Configuring Operator and Venue

Select a language preference, specifying the venue name and operator name, and click **OK**.

Describe the venue where the hotspot is located. If there are multiple hotspot APs in one venue, use the same venue name. However, when one hotspot covers multiple venues, you can list multiple venues here even though they may share a single service set identifier (SSID).

List venue names in multiple languages. The mobile device selects the language that is used to display information to the user. The mobile device can obtain venue name information through an ANQP query, which can help the user when they are manually selecting a hotspot. The mobile device implementation determines if the venue name information is displayed.

- 8 To remove a language row from the Venue list, select the checkbox in the list row and click the minus sign.

The screenshot shows the 'Hotspot Identification' tab. At the top, there are four tabs: 'Hotspot Identification' (selected), 'SP Identification', 'Network Characteristics', and 'Online Signup'. Below the tabs, there is a 'Domain:' text box. Underneath, 'Venue info:' has two dropdown menus: 'Assembly' and 'Stadium'. A table follows with the following data:

Language	Operator Name	Venue Name
<input checked="" type="checkbox"/>	English	John Doe
		Capital City Civic Center

To the right of the table, there are '+' and '-' buttons for adding and removing rows.

Figure 79: Removing a Venue

- 9 To edit a list row, click the list row. In the resulting dialog, modify the values and click **OK**.
- 10 Click **Save** to save the configuration.

SP Identification Tab

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

To configure SP Identification for the hotspot:

- 1 Configure a WLAN Services Hotspot. For more information, see [To Configure a New Hotspot](#) on page 329.
- 2 Select the **SP Identification** tab.

The screenshot shows the 'SP Identification' tab. At the top, there are four tabs: 'Hotspot Identification', 'SP Identification' (selected), 'Network Characteristics', and 'Online Signup'. Below the tabs, there are three main sections:

- NAI Realm:** A table with columns 'Realm' and 'EAP Method'. To the right are '+' and '-' buttons.
- Roaming Consortium:** Two text boxes labeled 'Entry 1: 0x' and 'Entry 2: 0x'.
- 3GPP Cellular Network:** Two text boxes labeled 'MCC' and 'MNC'. To the right is a '+' button.

A vertical scrollbar is visible on the right side of the configuration area.

Figure 80: Service Provider Identification

3 Configure the following parameters:

NAI Realm. The the NAI (Network Access Identification) Realms list is a FQDN of the service provider. This is a list of realms that can be successfully authenticated. Each realm may have up to 8 supported EAP methods. Click the plus sign to add realms and select the EAP Method. Then, click **OK**.

Configure an NAI Realm list for each hotspot as follows:

- Add all realms that can authenticate a mobile device's logon credentials or certificate credentials, including the realms of all roaming partners that are accessible from the hotspot AP. Include the realm of the home SP.
- Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information. See [Figure 82](#) on page 335
- You can configure the EAP method list to support devices that do not know the EAP methods that are being used by a given service provider.

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



Note

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

Realm Configuration

Realm:

EAP Methods:

<input type="checkbox"/> EAP-TTLS PAP	<input type="checkbox"/> EAP-TTLS CHAP
<input type="checkbox"/> EAP-TTLS MSCHAP	<input type="checkbox"/> EAP-TTLS MSCHAPv2
<input type="checkbox"/> EAP-TLS SIM	<input type="checkbox"/> EAP-SIM SIM
<input type="checkbox"/> EAP-AKA USIM	<input type="checkbox"/> EAP-AKA' USIM

OK Cancel

Figure 81: Realm Configuration

Mobile devices with a SIM or USIM credential, can obtain a realm from the hotspot NAI Realm list. While 3GPP credentials are usually used to access a hotspot, a targeted NAI home query is an efficient alternative approach. The device's connection manager compares the realm information in the list to the information that is stored on the device. The connection manager uses the mobile

device's preconfigured user preferences and policy to make a decision between a hotspot AP or a non-hotspot AP, if both are available.

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

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

3GPP Cellular Network. This is a list of cellular network IDs in the form of mobile country code, mobile network code (MCC, MNC). This list establishes whether an AP has a roaming arrangement with the 3GPP service providers. Click the plus sign to add mobile country code, mobile network code (MCC, MNC) values. Then, click **OK**.

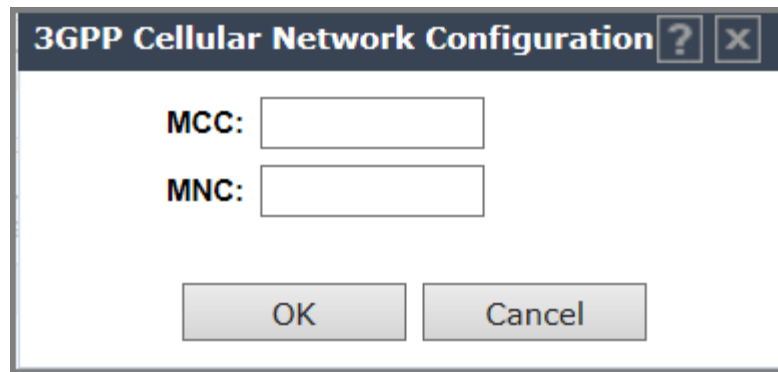


Figure 82: 3GPP Cellular Network Configuration

- 4 Click **Save** to save the configuration.

Network Characteristics Tab

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

To configure Network Characteristics for the hotspot:

- 1 Configure a WLAN Services Hotspot. For more information, see [To Configure a New Hotspot](#) on page 329.

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

Figure 83: Configuring Network Characteristics

- 3 Configure the following parameters:

IP Address Type Availability. The mobile device uses the IP Address Type Availability information to make network selection decisions. Select the level of restriction for each network type. Levels of restriction range from **Public Address Available** to **Port Restricted and Double NATed Private Address Available**.

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

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

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

- To add a protocol, click the plus sign. Specify the protocol, the port number, and the status associated with the protocol. Valid Status values include: Closed, Open, or Unknown.



Note

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

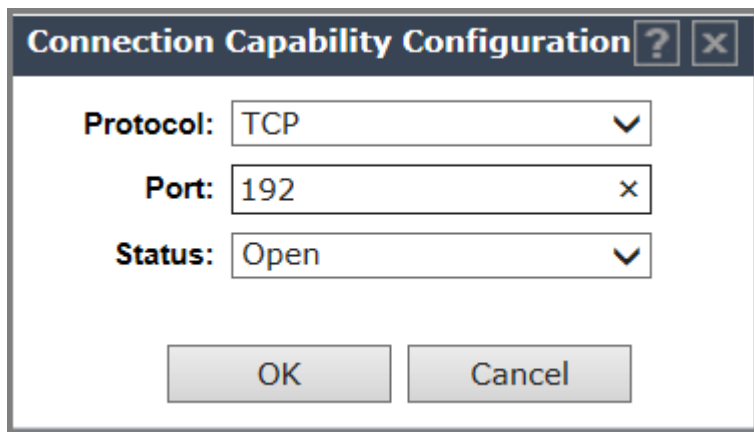


Figure 84: Configuring Connection Capability

- To remove a port from the Connection Capability list, select the checkbox in the list row and click the minus sign.

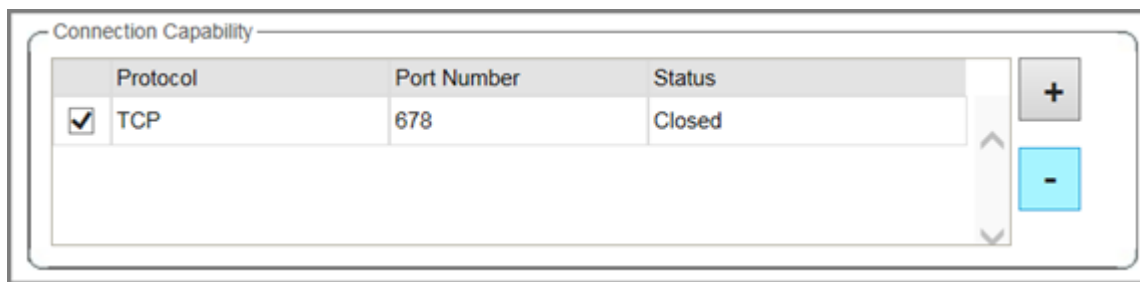


Figure 85: Removing a Connection Port

- To edit a port, click the list row. In the resulting dialog, modify the values and click **OK**.
- 4 Click **Save**.

Online Signup Tab

The hotspot Online Signup tab displays hotspot properties for Online Signup users. Online Signup allows users who are not part of the provider network to manually connect to the hotspot. It also allows for added security for users who want to connect anonymously.

To configure Online Signup for the hotspot:

- 1 Configure a WLAN Services Hotspot. For more information, see [To Configure a New Hotspot](#) on page 329.

- 2 Select the **Online Signup** tab.

Figure 86: Configuring Online Signup

- 3 Configure the following parameters:

Network Authentication Type. Possible values for network authentication are:

- Acceptance of terms and conditions. Redirection is accomplished after user accepts Terms and Conditions.
- Http/Https redirection. Redirect Http or Https automatically.
- Online enrollment supported. Authentication supports online enrollment.
- DNS redirection. DNS redirection serves a web page other than what the end user had requested.

OSU WLAN. This is the address of the Online Signup WLAN. When you created the hotspot, you specified OSU in [Step 1 above](#). The OSU WLAN can be either Open or Encrypted (OSEN).

Server Provider Setting. This is service provider configuration settings.

- To add a provider to the list, click the plus sign and configure the provider settings. For more information, see [Configuring the OSU Service Provider](#) on page 338.
- To remove a provider from the list, select the checkbox in the list row and click the minus sign.
- To edit provider information, click the list row. In the resulting dialog, modify the values and click **OK**. For more information, see [Configuring the OSU Service Provider](#) on page 338.

- 4 Click **Save** to save the configuration.

Configuring the OSU Service Provider

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

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

- 1 Configure a WLAN Services Hotspot. For more information, see [To Configure a New Hotspot](#) on page 329.

- From the WLAN Services Hotspot tab, select the **Online Signup** tab.

The screenshot shows a configuration window with four tabs: "Hotspot Identification", "SP Identification", "Network Characteristics", and "Online Signup". The "Online Signup" tab is active. Below the tabs, there are two dropdown menus: "Network Authentication Type" set to "Online enrollment supported" and "OSU WLAN" set to "osu". Below these is a "Service Provider Setting" section containing a table with columns: "Server URI", "Methods", "Icon", "Language", "Friendly Name", and "Description". The table is currently empty. To the right of the table are two buttons: a plus sign (+) for adding a new entry and a minus sign (-) for deleting an entry. At the bottom of the window are three buttons: "New", "Delete", and "Save".

Server URI	Methods	Icon	Language	Friendly Name	Description
------------	---------	------	----------	---------------	-------------

Figure 87: Online Signup Tab

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

OSU SP Configuration

Server URI:

Methods:

<input type="checkbox"/>	OMA DM	▲
<input type="checkbox"/>	SOAP XML SPP	▼

ICON:

Anonymous Name:

Language 1

Language:

Friendly Name:

Service Description:

Language 2

Language:

Friendly Name:

Service Description:

Figure 88: Configuring the OSU Service Provider

- 4 Configure the following parameters:

Server URI. The OSU server URI .

Methods. OSU Method is the preferred list of encoding methods that the OSU server supports in order of priority. Select the connection method used by the provider.

Icon. Click **Configure** to add or remove an icon associated with Online Signup. For more information, see [Configuring an OSU Icon](#) on page 341.

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

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

- 5 Click **OK** to save the OSU SP configuration.

Configuring an OSU Icon

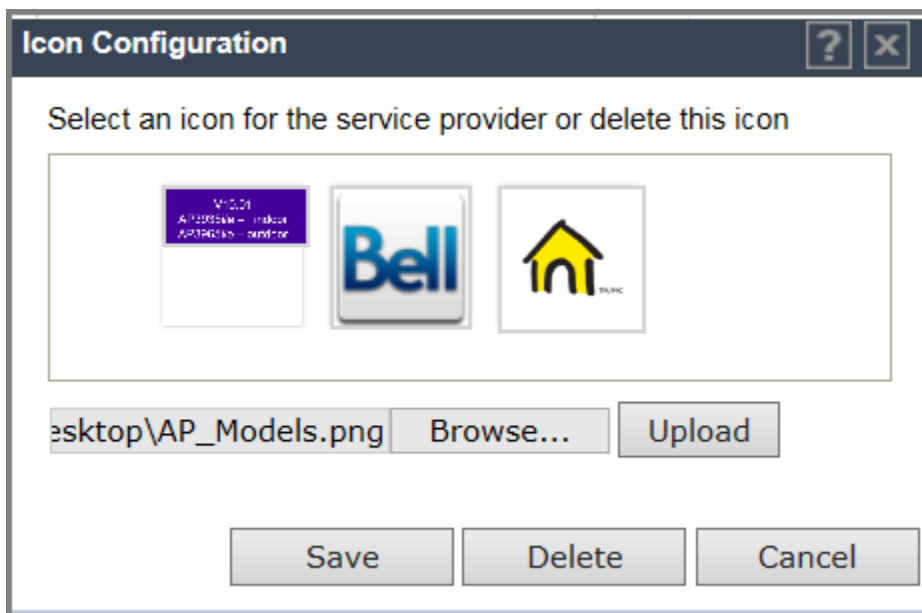
This task outlines how to add, change, or remove icons to a list of icons that are associated with Online Signup. The icon list contains the metadata for the available icon files. The metadata defines the image size, language, type, and file name. The mobile device determines which icon in the list best fits the display and downloads the appropriate file. The list can be blank.

The NAI realm is used in cases where the OSU ESS (OSEN) SSID is configured. This allows the device to authenticate to the OSU OSEN SSID for access to the OSU server.

To add an icon:

- 1 From the **OSU SP Configuration** dialog, click **Configure**.

The **Icon Configuration** dialog appears.



- 2 Click **Browse** to navigate to the icon file. Then, click **Open** and **Upload**.

The icon file is added to the **Icon Configuration** dialog.

- 3 Select the icon and click **Save**.

To delete an icon:

- 1 Open the **Icon Configuration** dialog.
- 2 Select the icon and click **Delete**.
- 3 Click **Save**.

8 Configuring a VNS

Configuring a VNS
VNS Global Settings
Methods for Configuring a VNS
Manually Creating a VNS
Creating a VNS Using the Wizard
Enabling and Disabling a VNS
Renaming a VNS
Deleting a VNS

Configuring a VNS

Setting up a VNS defines a binding between a default role specified for wireless users and an associated WLAN Service set, as shown in [Figure 89](#).

There are conceptually hierarchical dependencies on the configuration elements of a VNS. However, the provisioning framework is flexible enough that you may select an existing dependent element or create one on the fly. Therefore, each element can be provisioned independently (WLAN services, Topologies, and Roles). For service activation, all the pieces will need to be in place, or defined during VNS configuration.

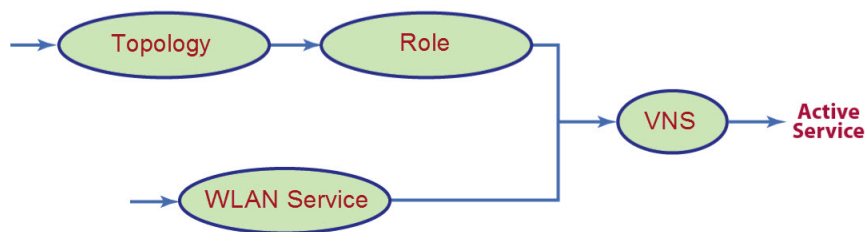


Figure 89: VNS Configuration Flow

You can use the VNS Creation Wizard to guide you through the necessary steps to create a virtual network service (and the necessary subcomponents during the process). The end result is a fully resolved set of elements and an active service.

The recommended order of configuration events is:

- 1 Before you begin, draft out the type of services the system is expected to provide — wireless services, encryption types, infrastructure mapping (VLANs), and connectivity points (switch ports). Switch port VLAN configuration/trunks must match the controller's.
- 2 Set up basic controller services such as NTP, Routing, DNS, and RADIUS Servers, using one of the following methods:

- Run the **Basic Configuration Wizard**, or
 - Manually define the necessary infrastructure components such as RADIUS Servers. RADIUS Servers are defined via the **VNS > Global > Authentication**.
- 3 Define Topologies. Topologies represent the controller's points of network attachment. Therefore, VLANs and port assignments need to be coordinated with the corresponding switch ports.
 - 4 Define Roles. Roles are typically bound to Topologies. Role application assigns user traffic to the corresponding network point of attachment.
 - Roles define mobile user access rights by filtering.
 - Policies reference the mobile user's traffic rate control profiles.
 - 5 Define the WLAN Service.
 - Define SSID and privacy settings for the wireless link.
 - Select the set of APs and Radios on which the service is present.
 - Configure the method of credential authentication for wireless users (None, Internal CP, External CP, Guest Portal, 802.1x[EAP]).
 - 6 Create a **VNS** that binds the **WLAN Service** to the **Role** that will be used for default assignment upon user network attachment.

The VNS configuration page in turn allows for in-place creation of any dependencies it may require. For example:

- Create a new WLAN Service.
- Create a new Role.
 - Create a new Topology.
 - Create a new Class of Service.

Controller Defaults

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

The ExtremeWireless system does ship with Topology entities representing each of its physical interfaces, plus an admin interface.

The controller system ships with a Topology entity for an admin interface. Topology entities representing the controller physical interfaces must be set manually or using the basic installation wizard.

There are, however, global default settings corresponding to:

- A Default Topology named "Bridged @ AP Untagged"
- An "Unlimited" Rate Control Profile
- A Filter Definition of "Deny all"

These entities are simply placeholders for Role completion, in case roles are incompletely defined. For example, a Role may be defined as "no-change" for Topology assignment.

If an incomplete Role is assigned as the default for a VNS / WLAN Service (wireless port), the incomplete Role needs to be fully qualified, at which point the missing values are picked from the Default Global Role definitions, and the resulting role is applied as default.



Note

You can edit the attributes of the Default Global Role (in the VNS > Globals tab) to any other parameters of your choosing (for example, any other topology, more permissive filter sets, more restrictive Rate Control profile).

It is possible to define a Default Global Role to refer to a specific Topology (for example, Topology_VLAN), and then configure every other Role's topology simply as "No-change." This will cause the default assignment to Topology_VLAN, so that all user traffic, regardless of which role they're currently using (with different access rights, different rate controls) will be carried through the same VLAN.

VNS Global Settings

Before defining a specific VNS, define the global settings that apply to all VNS definitions. These global settings include:

- Authentication
 - Configuring RADIUS servers on the enterprise network. The defined servers are displayed as available choices when you set up the authentication mechanism for each WLAN Service.
 - Configuring the MAC format.
 - Configuring RFC 3580 (ACCESS -ACCEPT) RADIUS attributes for the selected server. A Role Map Table maps each VLAN ID to a Role ID.
- DAS (Dynamic Authorization Service)
 - Configuring Dynamic Authorization Service (DAS) support. DAS helps secure your network by providing the ability to disconnect a mobile device from your network.
- Wireless QoS, comprising Admission Control Thresholds and Flexible Client Access Fairness Role.
 - Admission control thresholds protect admitted traffic against overloads, provide distinct thresholds for VO (voice) and VI (video), and distinct thresholds for roaming and new streams.
 - Flexible Client Access provides the ability to adjust media access fairness in five levels between Packet Fairness and Airtime Fairness.
- Bandwidth Control
 - The Bandwidth Control Profiles you define are displayed as available choices in the Rate Profiles menu when you set up role.
- Default Role

The Global Default Policy specifies:

- A topology to use when a VNS is created using a role that does not specify a topology
- A set of filters

The controller ships from the factory with a default "Global Default Policy" that has the following settings:

- Topology is set to an Bridged at AP untagged topology. This topology will itself be defined in controllers by default.
- Filters - A single "Allow All" filter.

The Global Default Policy is user-configurable. Changes to the Global Default Policy immediately effect all shadow roles created from it, just as if the administrator had made a comparable change directly to the incomplete role.

- Egress Filtering Mode

The global Egress Filtering Mode setting overrides the individual WLAN service Egress Filtering Mode setting.

- Sync Summary

The **Sync Summary** screen provides an overview of the synchronization status of paired controllers. The screen is divided into sections: Virtual Networks, WLAN services, Roles, and Topologies. Each section lists the name of the corresponding configuration object, its synchronization mode, and the status of last synchronization attempt. For more information, see [Using the Sync Summary](#) on page 365.

- NAC Integration

NAC Integration provides a list of NAC servers for use by the controller for passing traffic. The NAC server can accept DHCP messages from the controller's DHCP server and use them to fingerprint devices. For more information, see [Using NAC Integration](#) on page 367.

- Client Auto Login

This features configures how auto login behavior is handled for users with devices that need to authenticate to a captive portal to gain network access. For more information, see [Using Client Login](#) on page 368.

- Topology Group Algorithm

Topology Group Algorithms are used for selecting a member Topology from a Topology Group. The wireless controller will run one of the following algorithms: MAC based, Round Robin, Random Selected, and Lease used. For more information, see [Using Topology Group Algorithm](#) on page 369.

- Netflow/MirrorN

Use Netflow to forward packet information. Integration with ExtremeAnalytics no longer requires Netflow/MirrorN. See [ExtremeAnalytics Support with Enhanced IPFIX Records](#) on page 371 for more information.

- Redirection URL

Configure a list of redirection URLs from the Redirection URL dialog. You can add and delete a URL.



Note

To display the **Redirection URL** option, enable **Rule-based Redirection** under **Filtering Mode**.

Defining RADIUS Servers and MAC Address Format

The Authentication global settings include configuring RADIUS servers, the MAC format to be used, the SERVICE-TYPE attribute in the client ACCESS-REQUEST messages, and how long a notice Web page displays if a topology change occurs during authentication. The notice Web page indicates that authentication was successful and that the user must restart the browser to gain access to the network.

Defining RADIUS Servers for VNS Global Settings

To Define RADIUS Servers for VNS Global Settings:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global** > **Authentication**.
- 3 Select **Strict Mode** to force the top three Radius servers in priority order for each WLAN where applicable. Clearing this check box, allows individual Radius change per WLAN.

The screenshot displays the VNS configuration interface for Global Authentication Settings. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. The left sidebar shows a tree view with 'Global' selected, containing sub-items like Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, and Netflow/MirrorN. The main content area is titled 'RADIUS Servers' and includes a sub-section for 'RFC 3580 (ACCESS-ACCEPT) Options'. A 'Strict Mode' checkbox is present and unchecked. Below it is a table with the following data:

	Server		Default	Retries		Timeouts		Ports		Priority	
	Alias	Hostname/IP	Protocol	Auth	Acct	Auth	Acct	Auth	Acct	Auth	Acct
<input type="checkbox"/>	192.168.3	192.168.3.158	PAP	3	3	5	5	1812	1813	1	1

Below the table, a note states: '* RADIUS servers which are currently associated with WLAN Service(s) cannot be removed'. There are 'New' and 'Delete Selected' buttons. The 'MAC Address' section includes a 'MAC Address Format' dropdown set to 'XXXXXXXXXXXX' and a note '(for MAC-Based authentication only)'. An 'Advanced...' button is also visible. A 'Save' button is located at the bottom right of the configuration area.

Figure 90: Global Authentication Settings

- 4 To define a new RADIUS server available on the network, click **New**. The **RADIUS Settings** dialog displays.

RADIUS Settings [?] [X]

RADIUS Server

Server Alias:
Hostname/IP:
Shared Secret:
Default Protocol: PAP

Authentication

Priority:
Total Number of Tries:
RADIUS Request Timeout: (seconds)
Port:

Accounting

Priority:
Total Number of Tries:
RADIUS Request Timeout: (seconds)
Interim Accounting Interval: (minutes)
Port:

Health Monitoring

Polling Mechanism: Authorize an actual new user
Test Request Timeout: (seconds)

Figure 91: RADIUS Server Settings

- 5 In the **Server Alias** field, type a name that you want to assign to the RADIUS server.



Note

You can also type the RADIUS server's IP address in the **Server Alias** box in place of a nickname. The RADIUS server will identify itself by the value typed in the **Server Alias** box in the RADIUS Servers drop down list on the **RADIUS Authentication** tab of the **Login Management** screen (**top menu > Wireless Controller > Login Management**). For more information, see [Configuring the Login Authentication Mode](#) on page 74.

- 6 In the **Hostname/IP** field, type either the RADIUS server's FQDN (fully qualified domain name) or IP address.



Note

If you type the host name in the **Hostname/IP address** box, the controller will send a host name query to the DNS server for host name resolution. The DNS servers must be appropriately configured for resolving the RADIUS servers' host names. For more information, see [Configuring DNS Servers for Resolving Host Names of NTP and RADIUS Servers](#) on page 92.

- 7 In the **Shared Secret** field, type the password that will be used to validate the connection between the controller and the RADIUS server.

To proofread your shared secret key, click Unmask. The password is displayed.



Note

You should always proofread your Shared Secret key to avoid any problems later when the controller attempts to communicate with the RADIUS server.

- 8 If desired, change the **Default Protocol** using the drop down list. Choices are PAP, CHAP, MS-CHAP, or MS-CHAP2.
- 9 If desired, change the pre-defined default values for **Authentication** and **Accounting** operations:
- Priority — default is 4.
 - Total number of tries — default is 3.
 - RADIUS Request timeout — default is 5 seconds.
 - For Accounting operations, the Interim Accounting Interval — default is 30 minutes. Setting the Interim Accounting Interval value to 0 results in no interims being sent.
 - Port — default Authentication port is 1812. Default Accounting port is 1813.
- 10 If desired, setup Health Monitoring by selecting a **Polling Mechanism** from the drop-down menu, and enter a **Test Request Timeout** (shown in seconds).
- 11 To save your changes, click **Save**. The new server is displayed in the **RADIUS Servers** list.



Note

The RADIUS server is identified by its Server Alias.

- 12 To edit an existing server, click the row containing the server. The **RADIUS Settings** window displays, containing the server's configuration values.
- 13 To remove a server from the list, select the checkbox next to the server, and then click **Delete Selected**. You cannot remove a server that is used by any VNS.

Configuring the Global MAC Address Format for Use with the RADIUS Servers

To configure the Global MAC Address Format for use with the RADIUS servers:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global**, then **Authentication**.
- 3 In the **MAC Address** area, select the **MAC Address Format** from the drop down list.
- 4 Click **Save** to save your changes.

Configuring Advanced RADIUS Servers Settings

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global > Authentication**.
- 3 In the **MAC Address** area, click **Advanced**.

Advanced [?] [X]

Include the Service-Type attribute in Client Access Request messages

Set Service-Type to Login *

* This is incompatible with using RADIUS for administrative access to the controller.

Delay for Client Message for Topology Change seconds

How should multiple RADIUS servers be used?

For authentication: ▾

Use MAC-Based Authentication MAC address format for user authentication and accounting via RADIUS

RADIUS Accounting *

Defer sending the accounting start request until the client's IP address is known.

* Disabling RADIUS accounting overrides the RADIUS accounting settings of individual WLAN Services. Enabling RADIUS accounting activates RADIUS accounting only in WLAN Services specifically configured to perform it.

Figure 92: Advanced RADIUS Server Settings

4 Configure the following parameters:

Table 64: Advanced Radius Settings

Field	Description
Include Service-Type attribute in Client Access Request messages	Select if the client RADIUS Access Request message includes the "Service-Type" attribute. If included, the attribute is set to "Framed" by default.
Set Service Type to Login	<p>If selected, the RADIUS "Service-Type" attribute of the client Access Request is set to "Login" (instead of "Framed").</p> <p>Note: RADIUS-based controller administrative access also sets the Service-Type attribute to "Login". Therefore, if you enable Service Type Login here, RADIUS-based administrative access is not allowed (and vice versa).</p>
Delay for Client Message for Topology Change	Defines a delay during client authentication when switching from one topology to another. This is relevant for Captive Portal authentication. The delay gives time for the client to be assigned an IP address for the new topology before browser redirection. Set the delay in seconds.
How should multiple RADIUS servers be used?	<p>Select an authentication option. The selection applies to all WLAN Services and to all sites on the EWC.</p> <ul style="list-style-type: none"> • Round-Robin. The server is selected on a round-robin basis starting at the top of the list of approved servers. The first server is used until it fails, and that pattern continues down the list. When the last server fails, then the first server is used again. • Primary-Backup. Select a primary failover server to have control over which server provides redundancy. When you select Primary-Backup, the RADIUS server assigned to the site or WLAN Service is the primary for the WLAN Service. All other RADIUS servers assigned to WLAN Service are backups for the primary and continue to be selected in a round-robin approach. For controllers in an availability pair, the Primary and Backup servers must be synchronized (enable "Synchronize System Configuration" in Availability setup) if the WLAN Services are synchronized. If the primary server has failed resulting in a backup server being used for authentication, the controller will periodically send a "Health Check" to the primary server to see if it has recovered. If the primary server has recovered, the controller starts using the primary server for all new authentications. All authentications in progress continue to use the backup server. This feature impacts client authentication (not RADIUS Accounting) in the configuration where multiple RADIUS servers are used for authentication of primary server with backup servers.

Table 64: Advanced Radius Settings (continued)

Field	Description
Use MAC-Based Authentication MAC address format for user authentication and accounting via RADIUS	<p>Allows the administrator to override the default MAC address colon-separated format (for example 00:11:22:33:44:55) with the Global Authentication MAC Address format for the following attributes:</p> <ul style="list-style-type: none"> • Calling-Station-Id attribute of the RADIUS packet • Called-Station-Id attribute (if Called-Station-Id is not overridden by Zone name) • AP BSSID Mac in one of the vendor attributes • User-Name attribute. <p>Note: This setting is enabled for new deployments. You must manually enable this setting for upgraded deployments.</p>
Radius Accounting	<p>Enabling RADIUS accounting activates RADIUS accounting only in WLAN Services specifically configured to perform it. Disabling RADIUS accounting overrides the RADIUS accounting settings of individual WLAN Services.</p>
Defer sending the accounting start request until the client's IP address is known	<p>Specify Authentication Behavior of RADIUS servers on Server Failure. If selected, the client RADIUS Accounting Request "start" command is not sent to the RADIUS server until the client IP address is known. By default, this option is not selected and the "start" command is sent once the client is authenticated.</p>

- 5 Click **Close** to close the **Advanced Settings** dialog.
- 6 Click **Save** to save your changes.

Changing the Display Time of the Notice Web Page

To Change How Long the Notice Web Page Displays If a Topology Change Occurs During Authentication:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global**, then **Authentication**.
- 3 In the **MAC Address** area, click **Advanced**.
- 4 In the **Delay for Client Message for Topology Change** field, specify how long, in seconds, the Web page is displayed to the client when the topology changes as a result of a role change.

The Web page indicates that authentication was successful and that the user must close all browser windows and then restart the browser for access to the network.

Currently this is supported for Internal Captive Portal, Guest Portal, and Guest Splash.

- 5 Click **Close**.
- 6 Click **Save** to save your changes.

Configuring RADIUS Attribute for Hybrid Role Mode

Hybrid Role mode (RFC 3580 Mapping mode) enables the wireless controller to separately assign different roles or topologies depending on a mobile station location. The following are available modes of operation:

- **RADIUS Filter-ID attribute** — Controller uses the topology assigned by the role and ignores the VLAN tunnel ID.
- **RADIUS Tunnel-Private-Group-ID attribute** — Controller selects a role for the station based on the VLAN tunnel ID and ignores the filter ID. When selected, a mapping table maps each VLAN ID to a role.
- **Both RADIUS Filter-ID and Tunnel-Private-Group-ID attribute** — Controller uses both the role identified in the filter ID and the topology associated with the VLAN tunnel ID.

**Note**

The selected mode of operation applies to all WLAN Services on the controller.

Defining RFC 3580 Mapping Mode for VNS Global Settings

To define RFC 3580 for VNS global settings:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global > Authentication**.
- 3 Click the **RFC 3580 (ACCESS-ACCEPT) Options** tab.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. The left sidebar shows a tree view with 'Global' selected, and 'Authentication' expanded. The main content area is titled 'RFC 3580 (ACCESS-ACCEPT) Options' and contains the following elements:

- Strict Mode
- A table with columns: Server (Alias, Hostname/IP), Default (Protocol), Retries (Auth, Acct), Timeouts (Auth, Acct), Ports (Auth, Acct), and Priority (Auth, Acct). The table contains one entry: 'r1' with Hostname/IP '1.1.1.22', Protocol 'PAP', Retries '3' for both Auth and Acct, Timeouts '5' for both Auth and Acct, Ports '1812' for Auth and '1813' for Acct, and Priority '1' for both Auth and Acct.
- A note: '* RADIUS servers which are currently associated with WLAN Service(s) cannot be removed'
- Buttons: 'New' and 'Delete Selected'
- MAC Address** section with a dropdown menu for 'MAC Address Format' showing 'XXXXXXXXXXXX' and the text '(for MAC-Based authentication only)'. An 'Advanced...' button is also present.
- A 'Save' button at the bottom right.

Figure 93: Authentication Settings

- 4 Select **RADIUS Filter - ID attribute** to assign both role and topology when the controller receives a RADIUS ACCESS-ACCEPT message. To save your changes, click **Save**.

- 5 Select **RADIUS Tunnel-Private-Group-ID attribute** to assign both role and topology (based on the VLAN ID to Role Mapping table selection) when the controller receives a RADIUS ACCESS-ACCEPT message.

RADIUS Servers | **RFC 3580 (ACCESS-ACCEPT) Options**

When the controller receives a RADIUS ACCESS-ACCEPT:

- RADIUS Filter-ID attribute**
The Filter-ID attribute in the RADIUS ACCESS-ACCEPT message assigns both role and topology.
- RADIUS Tunnel-Private-Group-ID attribute**
The Tunnel-Private-Group-ID in the RADIUS ACCESS-ACCEPT message assigns both role and topology based on the VLAN ID to Role Mapping table.
- Both RADIUS Filter-ID and Tunnel-Private-Group-ID attributes**
The Filter-ID attribute identifies the role to assign to the station. The Tunnel-Private-Group-ID identifies the topology to assign to the station.

Vlan ID Role Mapping

Vlan ID	Role
---------	------

- In the VLAN ID Role Mapping table, select an existing VLAN ID and Role.
- Click **New** to create a new mapping entry. In the **Add VLAN Role** dialog, enter a VLAN ID, and select a Role from the drop-down list.

Add VLAN Role [?] [X]

Vlan ID: (1-4094)

Role:

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

- 6 Select **Both RADIUS Filter-ID and Tunnel-Private-Group-ID attributes** to identify the role to assign to the station and the topology to assign to the station (based on the VLAN ID to Role Mapping table selection), when the controller receives a RADIUS ACCESS-ACCEPT message.

The screenshot shows the 'RADIUS Servers' configuration page. Under the 'RFC 3580 (ACCESS-ACCEPT) Options' section, there are three radio button options for 'When the controller receives a RADIUS ACCESS-ACCEPT:'. The third option, 'Both RADIUS Filter-ID and Tunnel-Private-Group-ID attributes', is selected. To the right, there is a 'Vlan ID Role Mapping' table with columns for 'Vlan ID' and 'Role'. Below the table are 'New' and 'Delete Selected' buttons.

- In the VLAN ID Role Mapping table, select an existing VLAN ID and Role.
- Click **New** to create a new mapping entry. In the **Add VLAN Role** dialog, enter a VLAN ID, and select a Role from the drop-down list.

The 'Add VLAN Role' dialog box is shown. It has a title bar with a question mark and a close button. The 'Vlan ID' field is empty, with '(1-4094)' indicating the valid range. The 'Role' dropdown menu is set to 'data1AuthPolicy'. At the bottom, there are 'Add' and 'Cancel' buttons.

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

Configuring Dynamic Authorization Server Support

DAS helps secure your network by forcing the disconnection of any mobile device from your network. Typically, you would want to disconnect any unwelcome or unauthorized mobile device from your network. The “disconnect message” that is defined in RFC 3576 is enforced by the DAS support. If an unauthorized mobile device is detected on the network, the DAS client sends a disconnect packet, forcing the mobile device off the network. Your DAS client can be an integration with ExtremeControl or another third-party application, including RADIUS applications. For more information, see [NAC Integration with the Wireless WLAN](#) on page 26.

DAS support is available to all physical interfaces of the controller, and by default DAS listens to the standard-specified UDP port 3799.

To Configure Dynamic Authorization Server Support:

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

The screenshot shows the 'Dynamic Authorization Server Configuration' page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar has a 'New...' button and a list of categories: 'Global' (selected), 'Authentication', 'DAS', 'Wireless QoS', 'Bandwidth Control', 'Default Role', 'Egress Filtering Mode', 'NAC Integration', 'Client Autologin', 'Topology Group Algorithm', 'Netflow/MirrorN', and 'Redirection URL'. Below these are sections for 'Sites', 'Virtual Networks', 'WLAN Services', 'Roles', 'Classes of Service', and 'Topologies'. The main configuration area has two input fields: 'Port' with the value '3799' and 'Replay Interval' with the value '300' and the unit 'seconds'. A 'Save' button is located at the bottom right of the configuration area.

Figure 94: Global DAS Settings

- 3 In the **Port** box, type the UDP port you want DAS to monitor. By default, DAS is configured for the standard-specified UDP port 3799. It is unlikely this port value needs to be revised.
- 4 In the **Replay Interval** box, type how long you want DAS to ignore repeated identical messages. By default, DAS is configured for 300 seconds.
This time buffer helps defend against replay network attacks.
- 5 To save your changes, click **Save**.

Defining Wireless QoS Admission Control Thresholds

Defining the wireless QoS global settings include the following:

- [Configuring QoS Admission Control Thresholds](#) on page 357
- [Configuring QoS Flexible Client Access](#) on page 358

Configuring QoS Admission Control Thresholds

To define Admission Control Thresholds for VNS Global Settings:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global** > **Wireless QoS**.

The screenshot displays the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A 'Logout' link is visible in the top right corner. The left sidebar shows a 'New...' section with 'Global' selected, and a list of configuration options including Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, Netflow/MirrorN, and Redirection URL. Below this are sections for Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main content area is titled 'Admission Control Thresholds' and contains the following settings:

- Max Voice (VO) BW for roaming streams: 80%
- Max Voice (VO) BW for new streams: 60%
- Max Video (VI) BW for roaming streams: 60%
- Max Video (VI) BW for new streams: 40%
- Max Best Effort (BE) BW for roaming streams: 40%
- Max Best Effort (BE) BW for new streams: 30%
- Max Background (BK) BW for roaming streams: 30%
- Max Background (BK) BW for new streams: 20%

A note below these settings states: 'Note: Settings only apply on APs serving QoS-enabled WLAN Service with Admission Control enabled'. Below this is the 'Flexible Client Access' section, which includes a 'Fairness Policy' dropdown menu set to '100% Airtime'. A 'Save' button is located at the bottom right of the configuration area.

Figure 95: Wireless QoS Settings

- 3 In the **Admission Control Thresholds** area, define the thresholds for the following:
 - **Max Voice (VO) BW for roaming streams** — The maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.
 - **Max Voice (VO) BW for new streams** — The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.
 - **Max Video (VI) BW for roaming streams** — The maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.
 - **Max Video (VI) BW for new streams** — The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.
 - **Max Best Effort (BE) BW for roaming streams** —
 - **Max Best Effort (BE) BW for new streams** —
 - **Max Background (BK) BW for roaming streams** — The maximum allowed background bandwidth on an AP for roaming streams.
 - **Max Background (BK) BW for new streams** — The maximum allowed background bandwidth on an AP for new streams.

These global QoS settings apply to all APs that serve QoS enabled VNSs with admission control.

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

Configuring QoS Flexible Client Access

This feature allows you to adjust client access role in multiple steps between “packet fairness” and “airtime fairness.”

- Packet fairness is the default 802.11 access role. Each WLAN participant gets the same (equal) opportunity to send packets. All WLAN clients will show the same throughput, regardless of their PHY rate.
- Airtime fairness gives each WLAN participant the same (equal) time access. WLAN clients’ throughput will be proportional to their PHY rate.



Note

Flexible Client Access may not work if Global Admission Controls for Voice and Video (Advanced QoS settings) are enabled. Enabling Flexible Client Access will cause the AP to reboot.

To define Flexible Client Access for VNS Global Settings:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- In the left pane, click **Global** > **Wireless QoS**.

Figure 96: Wireless QoS Settings

- In the **Flexible Client Access** area, select a role from the **Fairness Role** drop-down list. Choices range from 100% packet fairness to 100% airtime fairness.



Note

TSPEC must be disabled when using Flexible Client Access.

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

Working with Bandwidth Control Profiles

Bandwidth control limits the amount of bidirectional traffic from a mobile device. A bandwidth control profile provides a generic definition for the limit applied to certain wireless clients' traffic. A bandwidth control profile is assigned on a per role basis. A bandwidth control profile is not applied to multicast traffic.

A bandwidth control profile consists of the following parameters:

- **Profile Name** — Name assigned to a profile
- **Committed Information Rate (CIR)** — Rate at which the network supports data transfer under normal operations. It is measured in kilo bits per second (Kbps).

The bandwidth control profiles you define on the **Global Settings** screen are displayed as available choices in the **Bandwidth Control Profiles** list on the **Classes of Service** screen.

To Create a Bandwidth Control Profile:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global** > **Bandwidth Control**.

Figure 97: Global Bandwidth Control Settings

- 3 Create a bandwidth control profile by doing the following:
 - **Profile Name** — Type a name for the bandwidth control profile.
 - **In the Average Rate (CIR)** — Type the CIR value for the bandwidth control profile.
- 4 Click **Add Profile**. The profile is created and displayed in the **Bandwidth Control Profiles** list.
- 5 Create additional bandwidth control profiles, if applicable.
- 6 To save your changes, click **Save**.

Configuring the Global Default Policy

The controller ships with a Global Default Policy that can be configured. The Global Default Policy specifies:

- A topology to use when a VNS is created using a role that does not specify a topology. The default assigned topology is named Bridged at AP untagged.
- A set of filters.

Configuring the Topology and Rate Profiles

To Configure the Topology and Rate Profiles:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global > Default Role**.
- 3 Select the **VLAN & Class of Service** tab.

The screenshot shows the 'Role: Global Default Role' configuration page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar has 'Global' selected, with sub-items like 'Authentication', 'DAS', 'Wireless QoS', 'Bandwidth Control', 'Default Role', 'Egress Filtering Mode', 'NAC Integration', 'Client Autologin', 'Topology Group Algorithm', 'Netflow/MirrorN', and 'Redirection URL'. The main content area has two tabs: 'VLAN & Class of Service' and 'Policy Rules'. Under 'VLAN & Class of Service', there are three sections: 'Core' with 'Role Name: Global Default Role'; 'Default Action' with 'VLAN: Bridged at AP untagged(4093)' and 'Edit'/'New' buttons; and 'Invalid Role Action' with radio buttons for 'Apply VNS Default Role' (selected), 'Allow All traffic', and 'Deny All traffic'. A 'Save' button is at the bottom right.

Figure 98: Default Role Settings

- 4 In the **Default Action** area, select a VLAN using one of the following methods:
 - Select an existing VLAN from the drop-down list.
 - Select an existing VLAN from the drop-down list, then click **Edit**. The **Edit Topology** window displays, showing the current values for the selected topology.
 - Click **New**. The **New Topology** window displays.

Edit or create the selected topology as described in [Configuring a Basic Data Port Topology](#) on page 223.
- 5 Select an Invalid Role Action from the one of the following:
 - Select **Apply Default Role**.
 - Select **Allow All traffic**.
 - Select **Deny All traffic**.
- 6 Click **Save**.

Configuring the Filters

To Configure the Filters:

- 1 Click the **Policy Rules** tab. The **Rules** tab displays, allowing you to create policy rules that will be applied by the controller when default non-authentication role does not specify filters.

Role: Global Default Role

VLAN & Class of Service | Policy Rules

Rules | Custom AP rules | AP Filtering | Custom AP Rules

In	Out	EthType	MAC	IP : Port	Protocol	Priority	ToS/DSCP	Access
dest	none	Any	Any	0.0.0.0/0	Any	Any	N/A	Allow
none	src	Any	Any	0.0.0.0/0	Any	Any	N/A	Allow

Add Edit Delete Up Down Top Bottom

* Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters instead.

Save

Figure 99: Default Role Settings

- 2 To add a rule, click **Add**.
- 3 For more information, see [Policy Rules](#) on page 243.
- 4 To configure custom AP filters, select **AP Filtering** and **Custom AP Rules** then click the **Custom AP rules** tab.

For more information, see [Defining Policy Rules for Wireless APs](#) on page 253.

Related Links

[Understanding the Filter Rule Definition Dialog](#) on page 257

[L7 Configuration](#) on page 262

Configuring Egress Filtering Mode

The controller can be configured to support Policy Manager's Egress Role mode. Egress Role refers to taking the ingress filters assigned to a port, exchanging the source and destination addresses with each other in each role rule and applying the result to the traffic egressing the port.

The ExtremeWireless solution applies egress filtering mode to WLAN services. When egress filtering is enabled, any role that is applied to a station on the WLAN service will have its outbound filters replaced with rules in which the source and destination addresses of the inbound filters are swapped.

The same role can be assigned to stations on WLAN services that have egress filtering mode enabled and on WLAN services that have it disabled.

- For stations that are on WLAN services with egress filtering mode enabled, the roles outbound filters will be replaced by ones derived from the inbound policy rules.
- For stations that are on WLAN services with egress filtering disabled, the outbound filters of the role will be applied as defined. In other words the same role can be applied in two different ways at the same time, based on the egress filter mode settings of the WLAN services it is used with.

The global Egress Filtering Mode setting overrides the individual WLAN service Egress Filtering Mode setting. By default, the global setting is set to **Use WLAN**. In this mode, egress filtering can be enabled for some WLAN services and not others. Set the Egress Filtering Mode setting from the Advanced configuration dialog of each WLAN service.

Changing the global setting does not alter each individual WLAN egress filtering mode setting, although the global setting can override the individual setting. Changing the global setting does not alter the outbound policy rules of each role. Each role's policy rules are stored on the controller as they were entered. Changing the global egress filtering mode flag does, however, affect how a role's rules are interpreted when they are applied.

Rule-Based Redirection

Rule-based redirection requires explicit enablement. For new installations, Rule-based Redirection is enabled by default. For upgrades from releases prior to v10.11, ExtremeWireless preserves the previous captive portal redirection method of triggering redirect off denied HTTP/HTTPS for non-authenticated roles. For more information, see [Rule-Based Redirection](#) on page 244.



Note

The option to disable Rule-based Redirection is available for backward capability only.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), and Radar. On the left, a sidebar menu lists various configuration options, with 'Filtering Mode' highlighted in a red box. The main content area is titled 'Egress Filtering Mode Configuration' and contains three radio button options: 'All WLAN Services enforce explicitly defined "Out" rules', 'All WLAN Services apply "In" filter rules to "Out" direction traffic *', and 'Use WLAN Service setting' (selected). Below this, a section titled 'Rule Based Redirection' is highlighted with a red box, containing a checked checkbox for 'Enable Rule Based Redirection'.

Figure 100: Enabling Rule-based Redirection

Related Links

[Configuring the In/Out Rules for WLAN Services Settings](#) on page 364

[Rule-Based Redirection](#) on page 244

Configuring the In/Out Rules for WLAN Services Settings

To configure the Egress Filtering Mode:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global > Filtering Mode**. The **Egress Filtering Mode Configuration** screen displays.

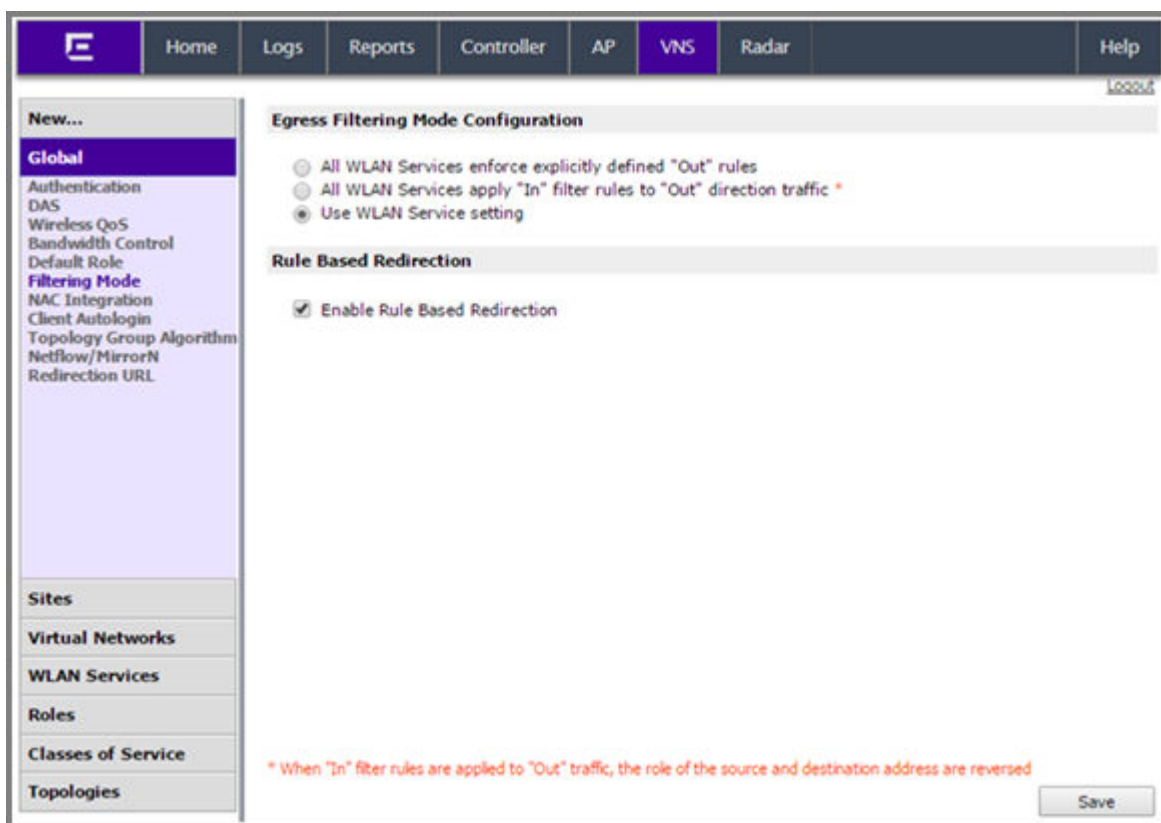


Figure 101: Egress Filtering Mode

- 3 Select an egress filtering mode:
 - **All WLAN Services enforce explicitly defined “Out” rules** – All WLAN services enforce outbound filters on egress traffic exactly as they are defined in the role.
 - **All WLAN Services apply “In” policy rules to “Out” direction traffic** – All WLAN services enforce that outbound policy rules that are explicitly defined in the role are overridden by a set of rules created by copying each inbound role rule and swapping the source and destination address roles in the rule.
 - **Use WLAN Service setting** – Each role’s rules are interpreted in accordance with the **Egress Filtering Mode** setting of each WLAN Service on which the role is applied. In this mode, it is possible that a role’s rules can be interpreted in two different ways at the same time, if it is used simultaneously on a WLAN service that has **Enforce explicitly defined “Out” rules** enabled and on a WLAN service that has **Apply “In” rules to “Out” direction traffic** at the same time.

Note



The **Use WLAN Service setting** is recommended. If you are using Policy Manager, configure each WLAN Service’s Egress filtering option directly from Policy Manager. Enabling Egress Filtering on a WLAN Service port in Policy Manager is equivalent to setting **Apply “In” rules to “Out” direction traffic** in the **WLAN Service’s Advanced** dialog.

- 4 Select **Rule-based Redirection** to enable redirection based on configured policy rules after a packet is denied. For more information, see [Rule-Based Redirection](#) on page 244.

Upgrade considerations for default Rule-based Redirection setting:

- This setting is enabled for the following installation scenarios:
 - For new installations of ExtremeWireless v10.11 or later
 - When upgrading from ExtremeWireless v10.11 or later
 - For factory resets of ExtremeWireless v10.11 or later
- When upgrading from a previous version of ExtremeWireless, this checkbox is cleared, and Rule-based Redirection is disabled.

Related Links

[Configuring Egress Filtering Mode](#) on page 362

[Rule-Based Redirection](#) on page 244

[Managing Redirection URLs](#) on page 372

Using the Sync Summary

The **Sync Summary** screen provides an overview of the synchronization status of paired controllers.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A Logout link is in the top right. A left sidebar contains a 'New...' menu with options: Global (selected), Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, Sync Summary, NAC Integration, and Client Autologin. Below this are sections for Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies.

The main content area is divided into sections:

- Global:** A checkbox for 'Synchronize System Configuration' is checked.
- Global Settings [Hide]:** A table with one row: Global Settings | Synchronized.
- Sites [Hide]:** A table with three rows:

Name	Sync	Status
dshjkal	<input checked="" type="checkbox"/>	Synchronized
gfdsgf	<input checked="" type="checkbox"/>	Synchronized
site3	<input checked="" type="checkbox"/>	Synchronized
- Virtual Networks [Hide]:** A table with four rows:

Name	Sync	Status
C100-01-Open	<input checked="" type="checkbox"/>	Synchronized
C100-02-WEP	<input checked="" type="checkbox"/>	Failed
C100-03-WPA-PSK	<input checked="" type="checkbox"/>	Synchronized
C100-04-WPA-PSK	<input type="checkbox"/>	Failed

A 'Save' button is located at the bottom right of the main content area.

The screen is divided into five sections: Virtual Networks, WLAN services, Roles, Classes of Service, and Topologies. Each section lists the name of the corresponding configuration object, its synchronization mode, and the status of last synchronization attempt.

If Synchronization of an object is not enabled, then there is a button in the Status field which says “Synchronize Now”, which performs a single synchronization of the object, pushing the object from local controller to the peer.

If Synchronization of an object is enabled, then the “Status” field can have the following values:

- Synchronized
- Not Synchronized
- Failed
- Conflict (with a button called “Resolve”)

The **Synchronize System Configuration** checkbox acts as a global synchronization flag. When it’s disabled, synchronization is not performed in the background. When it is enabled, only the objects that have “Sync” enabled are synchronized.

An object may have a synchronization state of “Conflict” if it was updated on both controllers in the availability pair while the availability link was down. In such a case, the **Resolve** button lets you choose which version of the object should be taken, local or remote. Please note that controllers don’t compare the actual configuration when they declare a conflict – only the fact that the object was updated on both controllers in the availability pair triggers the “Conflict” state.

Using NAC Integration

NAC Integration provides the ability to forward traffic from a controller to a configured NAC server. When a controller is configured to be a topology's DHCP server, or a relay for a topology, and this feature is enabled, traffic is forwarded to the NAC server. The NAC Integration Options screen provides a list of NAC servers that will accept DHCP messages from the controller. A maximum of three address can be entered and only one address can be entered for each NAC Server. To stop DHCP forwarding, all configured NAC servers need to be deleted from the list. The screen lists the NAC Server, NAC Name and IP Address. The screen provides the ability to add a new server or delete an existing entry.

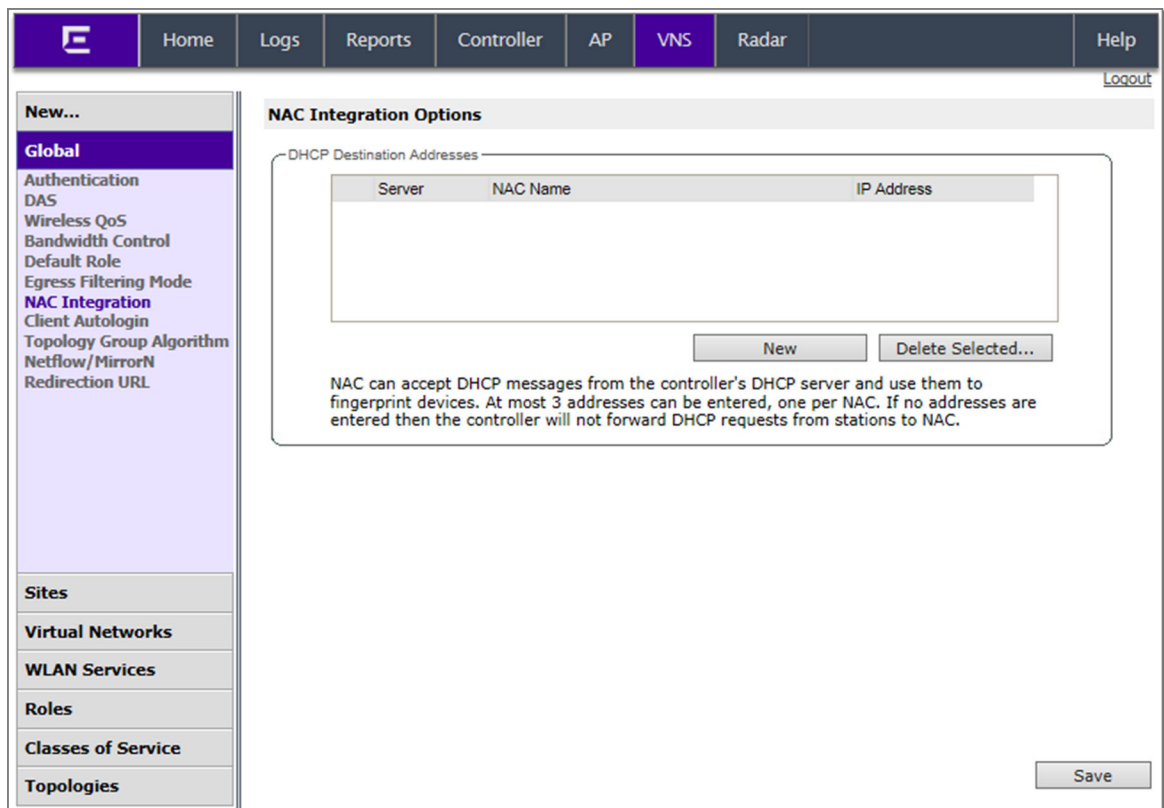
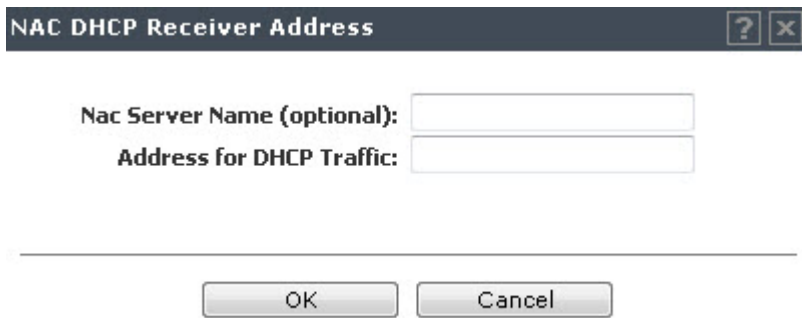


Figure 102: NAC Integration Settings

Adding a New NAC Server Destination

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global > NAC Integration**.

- 3 Click **New**. The **NAC DHCP Receiver Address** dialog appears.



The screenshot shows a dialog box titled "NAC DHCP Receiver Address". It has a dark header bar with a question mark icon and a close button (X). Below the header, there are two text input fields. The first is labeled "Nac Server Name (optional):" and the second is labeled "Address for DHCP Traffic:". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

- 4 For **Nac Server Name**, enter a name for the NAC Server. This is an optional step, but it helps to identify a specific server.
- 5 For **Address for DHCP Traffic**, enter the IPv4 address for Traffic.
- 6 Click **OK**.

Using Client Login

When a client uses a device that provides autologin capabilities, an attempt is made to detect whether the device needs to authenticate to a captive portal to gain network access via the controller. If the device determines that captive portal authentication is required, a login dialog is displayed. After logging in, access is granted and the browser window closes.

This autologin behavior is incompatible with deployments that need to direct all wireless users to a specific web page after the login completes. Using the Client Autologin feature provides configuration options to control autologin behavior.

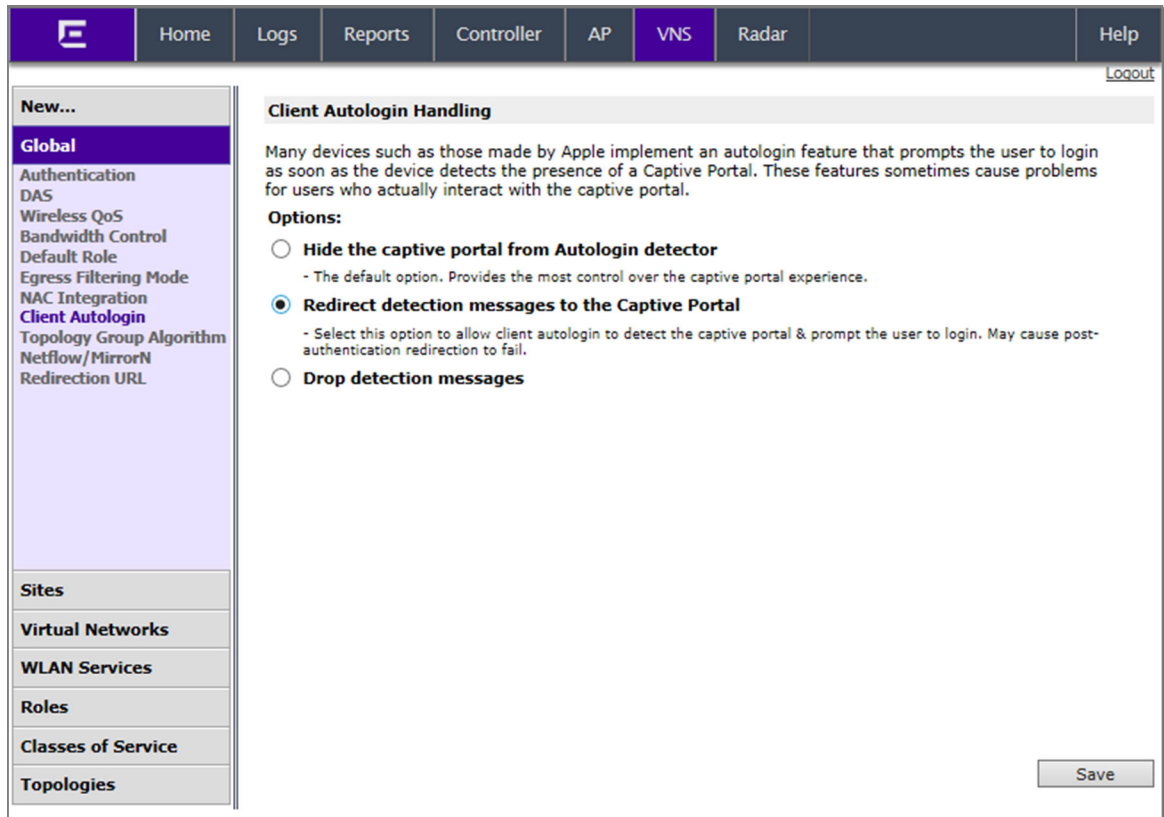


Figure 103: Global Client Autologin

Selecting a Client Autologin Option

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global > Client Autologin**.
The **Client Autologin Handling** screen displays.
- 3 Select from one of the following options:
 - When Autologin is set to **Hide the captive portal from Autologin detector**, the server is spoofed and creates the impression that there is no captive portal. This is the default option.
 - When Autologin is set to **Redirect detection messages to the Captive Portal**, the client detects the captive portal and prompts the user to login.
 - When Autologin is set to **Drop detection messages**, the controller ignores the connection request and drops the client.
- 4 Click **Save** to save the desired option.

Using Topology Group Algorithm

Tunneled station traffic is forwarded from the AP to the controller as if the groups were plain topologies. The controller provides minimum support to use only tunneled topology groups (B@AC, routed). The controller will run the Topology Group Algorithm and will not forward the mapping table to the AP.

Topology Group Selection Algorithm

Algorithm for Selecting a Member Topology from a Topology Group

Options:

- MAC-Based**
 - Hash on selected bits of the MAC address mod the number of topologies in the topology group. This algorithm always assigns a client to the same topology within the topology group.
- Round Robin**
 - The list is considered ordered; start at the top of the list. The next assignment is the next topology on the list; wrap around at the bottom.
- Random Selected**
 - Random number selected from a uniform distribution mod the number of topologies in the topology group.
- Least Used**
 - Assign a topology in the topology group with the least number of stations assigned to it at the moment of assignment.

Figure 104: Topology Group Algorithm

The following algorithms are available for selecting a member topology from a Topology Group:

- **MAC-Based:** This algorithm always assigns a client to the same topology within the topology group.
- **Round Robin:** The list is considered ordered; start at the top of the list. The next assignment is the next topology on the list; wrap around at the bottom.
- **Random Selected:** Random number selected from a uniform distribution mod the number of topologies in the topology group.
- **Least Used:** Assign a topology in the topology group with the least number of stations assigned to it at the moment of assignment.



Using Netflow/MirrorN

Use Netflow to forward packet information. Integration with ExtremeAnalytics no longer requires Netflow/MirrorN. See [ExtremeAnalytics Support with Enhanced IPFIX Records](#) on page 371 for more information.

Logs	Reports	Controller	AP	VNS	Radar
Netflow/MirrorN Configuration					
Netflow Export-Destination IP Address:				<input type="text" value="0.0.0.0"/>	
Netflow Export Interval:				<input type="text" value="60"/> (30-360 seconds)	
Mirror first N:				<input type="text" value="15"/> (1-31 packets/flow)	
Traffic Mirror L2 Port:				<input type="text" value="None"/> ▼	

Figure 105: Netflow/MirrorN

The following configuration items are supported:

- **Netflow Export-Destination IP Address:** Configure the ExtremeAnalytics engine IP to receive Netflow records.
- **Netflow Export Interval:** Configure the Netflow sending interval for same flow. The default value is 60. It will support from 30 to 360 seconds.
 - **Mirror first N:** Configure the MirrorN first N packets. It is a global setting per controller and all APs (per link). Default setting is 15.
 - **Traffic Mirror L2 Port:**

Configure the mirror port on the controller. The default value is **None**. The other I2 ports can only be selected when it is not referred elsewhere (lag, topologies).



ExtremeAnalytics Support with Enhanced IPFIX Records

ExtremeWireless leverages and integrates with ExtremeAnalytics for decoding, detection, collection of Metadata, and scrutinization of Layer 7 data. The solution functions by first enabling WLANs on the wireless controller to forward packets to the ExtremeAnalytics engine. This feature requires ExtremeAnalytics 7.0.8 or later.

Depending on your topology, the controller and the AP can inspect the flow, generate the application ID and round trip time (RTT), and format the IPFIX record. With B@AP, the AP sends the IPFIX record to the controller via a WASSP tunnel and then the controller exports the record to ExtremeAnalytics. With B@AC, the controller exports the IPFIX record to ExtremeAnalytics directly.

The IPFIX packets provide all the standard information found in a Netflow v9 packet with enhanced IPFIX parameters. The standard packet includes source and destination IP addresses, ports, protocol, and packet counter information. The enhanced IPFIX records include the application group ID, display

ID, round trip times (RTT), and flow meta data (which is part of the URL to help classify the flow). The enhanced IPFIX records that the controller sends releases the dedicated MirrorN port and reduces ExtremeAnalytics CPU resources previously used to identify the application.

IPFIX record templates are supported for IPv4 and IPv6.

Upgrades retain NETFLOW configuration, delivering enhanced records. Netflow with IPFIX reporting is disabled by default.

Managing Redirection URLs

Configure a list of redirection URLs from the Redirection URL dialog. You can add and delete a URL.



Note

To display the **Redirection URL** option, enable **Rule-based Redirection** under **Filtering Mode**.

For more information, see [Configuring the In/Out Rules for WLAN Services Settings](#) on page 364.

The URL list can contain up to 255 proper URLs, consisting of Fully-Qualified Domain Name (FQDN) addresses and IPV4 addresses. Duplicate entries are not permitted, and you must ensure that network traffic is accessible to the required IP addresses. The name of the WLAN Service that these entries are created for is displayed on the user interface and on the command line interface. SNMP also displays the URLs when queried through the Policy Profile MIB.

External Captive Portal URLs are not required, but when they exist, they are automatically added to the list.



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 .

For URL specifications, see [Adding a Redirection URL](#) on page 372.

Related Links

[Configuring the In/Out Rules for WLAN Services Settings](#) on page 364

[Adding a Redirection URL](#) on page 372

[Deleting a Redirection URL](#) on page 373

Adding a Redirection URL

- 1 There are two ways to add a redirection URL:
 - Adding from the **Redirection URL** list, go to **VNS > Global > Redirection URL** and click **Add**.
 - Adding from the **VLAN & Class of Service** tab, go to **VNS > Roles > VLAN & Class of Service**. Beside the **Redirection URL** field, click **New**.

The **Redirection URL** dialog displays.

- 2 Enter the URL for redirection.

Redirection destinations have the following specifications:

- Only one redirection destination per role.
- The redirection destination is configurable and is comprised of one of the following items:
 - The IP address and port of the destination server. In this case, the redirection is driven by the HTTP Get query from the redirected request.
 - A complete URL. In this case, the redirection is driven by the HTTP Get query that the administrator specifies. Using the controller interface, you can augment the Get query with the following parameters:

Session identifier or token for the station of the redirected traffic

Address & port of the controller that is performing the redirection

Destination URL of the redirection. The default redirection destination is 'Own WLAN'.



Note

The default Redirection destination is 'Own WLAN'.

Related Links

[Managing Redirection URLs](#) on page 372

Modifying a Redirection URL

To modify a redirection URL:

Navigate to **VNS > Global > Redirection URL**, and click **Edit**.



Note

Changes made to an existing redirection URL affect all roles using that redirection URL.

Deleting a Redirection URL

To delete a redirection URL:

- 1 Navigate to **VNS > Global > Redirection URL**.



Note

To display the **Redirection URL** option, enable **Rule-based Redirection** under **Filtering Mode**. For more information, see [Configuring the In/Out Rules for WLAN Services Settings](#) on page 364.

- 2 Select the URL in the list to delete, and click **Delete Selected**.



Note

URLs that are in use, cannot be deleted from the list.

Methods for Configuring a VNS

To configure a VNS, you can use one of the following methods:

- **Manual configuration** — Allows you to create a new VNS by first configuring the topology, role, and WLAN services and then configuring any remaining individual VNS tabs that are necessary to complete the process.

When configuring a VNS, you can navigate between the various VNS tabs and define your configuration without having to save your changes on each individual tab. After your VNS configuration is complete, click Save on any VNS tab to save your completed VNS configuration.



Note

If you navigate away from the VNS configuration tabs without saving your VNS changes, your VNS configuration changes will be lost.

- **Wizard configuration** — The VNS wizard helps create and configure a new VNS by prompting you for a minimum amount of configuration information. The VNS is created using minimum parameters. The remaining parameters are automatically assigned in accordance with best practice standards.

After the VNS wizard completes the VNS creation process, you can then edit or revise any of the VNS configuration to suit your network needs.

Manually Creating a VNS

Advanced configuration allows administrators to create a new VNS once the topology, role, and WLAN services required by the VNS parameters are available. The topology, role and WLAN services could be created in advance or could be created at the time of VNS configuration.

When you create a new VNS, additional tabs are displayed depending on the selections made in the Core box of the main VNS configuration tab.

When configuring a VNS, you can navigate between the various VNS tabs and define your configuration without having to save your changes on each individual tab. After your VNS configuration is complete, click Save on any VNS tab to save your complete VNS configuration.



Note

If you navigate away from the VNS Configuration tabs without saving your VNS changes, your VNS configuration changes will be lost.

The following procedure lists the steps necessary to create a VNS in advanced mode. Each step references a section in this document that describes the full details. Follow the links provided to go directly to the appropriate sections.

Creating a VNS Manually

To create a VNS manually:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- In the left pane, expand the **Virtual Networks** pane and select an existing VNS to edit, or click **New**.

The screenshot shows the VNS configuration page for 'VNS: CNL-220-0-0'. The left sidebar contains a navigation menu with categories: New..., Global, Sites, Virtual Networks (selected), WLAN Services, Roles, Classes of Service, and Topologies. Under 'Virtual Networks', a list of VNS IDs is shown, with 'CNL-220-0-0' selected. The main content area is titled 'VNS: CNL-220-0-0' and has a 'General' tab. It is divided into four sections: 'Core' with a 'VNS Name' field containing 'CNL-220-0-0'; 'WLAN Service' with a dropdown menu set to 'CNL-220-0-0' and 'Edit' and 'New' buttons; 'Default Roles' with two rows: 'Non-Authenticated' (dropdown: 'CNL-220-0-0-non-authenticated', 'Action:4093 Class of Service:High ThroughPut') and 'Authenticated' (dropdown: 'CNL-220-0-0-default', 'Action:4093 Class of Service:High ThroughPut'), each with 'Edit' and 'New' buttons; and 'Status' with 'Synchronize' (checkbox checked, '[synchronized]', 'Replicated when Synchronize Configuration is enabled') and 'Enable' (checkbox checked). At the bottom are 'New', 'Delete', and 'Save' buttons.

Figure 106: VNS Settings

- Enter a name for the VNS.
- Select an existing WLAN Service for the VNS, or create a new WLAN Service, or edit an existing one.
For more information, see [Configuring a Basic WLAN Service](#) on page 274.
- Configure the Default Roles for the VNS. Select existing roles, or create new roles, or edit existing ones.
For more information, see [Configuring a VNS](#) on page 343.
- Configure the Status parameters for the VNS:
 - Synchronize** — Enable automatic synchronization with its availability peer. Refer to [Using the Sync Summary](#) on page 365 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable this feature.
 - Enabled** — Check to enable the VNS.
- Click **Save** to save your changes.

Also, as with creating a new VNS, you can:

- Configure a topology for the VNS
- Configure a role for the VNS
- Configure WLAN services for the VNS
- Configure additional roles for the VNS

Creating a VNS Using the Wizard

The VNS wizard helps create and configure a new VNS by prompting you for a minimum amount of configuration information during the sequential configuration process. After the VNS wizard completes the VNS creation process, you can then continue to configure or revise any of the VNS configuration to suit your network needs.

When using the VNS wizard to create a new VNS, you can create the following types of VNSs:

- **NAC SSID-based VNS** — NAC gateway-compatible VNS. The controller integrates with an Extreme Networks NAC Controller to provide authentication, assessment, remediation and access control for mobile users. For more information, see [Creating a NAC VNS Using the VNS Wizard](#) on page 376.
- **Voice** — Voice-specific VNS that can support various wireless telephones, including optiPoint, Spectralink, Vocera, and Mobile Connect - Nokia. For more information, see [Creating a Voice VNS Using the VNS Wizard](#) on page 378.
- **Data** — Data-specific VNS, that can be configured to use either SSID or AAA authentication. For more information, see [Creating a Data VNS Using the VNS Wizard](#) on page 386.
- **Captive Portal** — A VNS that employs a Captive Portal page, which requires mobile users to provide login credentials when prompted to access network services. In addition, use the VNS wizard to configure a GuestPortal VNS using the Captive Portal option. For more information, see [Creating a Captive Portal VNS Using the VNS Wizard](#) on page 396.

The VNS type dictates the configuration information that is required during the VNS creation process.

Creating a NAC VNS Using the VNS Wizard

The ExtremeWireless controller integrates with an Extreme Networks NAC controller to provide authentication, assessment, remediation and access control for mobile users. For more information, see [NAC Integration with the Wireless WLAN](#) on page 26.

Use the VNS wizard to configure a NAC gateway-compatible VNS by defining the following essential parameters:

- **VNS Name** — The name that will be assigned to the VNS and SSID.
- **IP Address** — The IP address of the ExtremeWireless controller's interface on the VLAN.
- **Mask** — The subnet mask for the IP address to separate the network portion from the host portion of the address.
- **VLAN ID** — ID number of the VLAN to which the ExtremeWireless controller is bridged for the VNS.
- **Port** — Physical L2 port to which the configured VLAN is attached.
- **RADIUS server** — IP address of the NAC controller.
- **Redirection URL** — The URL that points to the NAC controller's web server.

The VNS wizard creates a Bridge Traffic Locally at EWC VNS. This VNS has the crucial attributes — SSID Network Assignment Type, MAC-based external captive portal authentication and WPA-PSK encryption — that makes it compatible with the NAC controller. The remaining VNS parameters are defined automatically according to best practice standards.

To configure a NAC VNS using the VNS wizard:

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

- 2 In the left pane, click **New > START VNS WIZARD**.

VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

Name:

Category:

(Next: Basic Settings)

Back Next Cancel

- 3 In the **Name** box, type a name for the NAC SSID-based VNS.
- 4 In the **Category** drop-down list, click **NAC VNS**, and then click **Next**.

NAC-compatible VNS

This wizard enables you to quickly configure a NAC-compatible VNS by entering the essential settings only. The other settings are filled in automatically according to best practice standards.

VNS Name:

IP Address:

Mask:

Interface:

VLAN ID:

NAS:

NAC server: (for MAC-based auth) Use existing server Add new server

Server Alias:

Hostname/IP:

Shared Secret: Unmask

NAC web server IP:

Back Finish Cancel

Table 65: NAC-compatible VNS Page - Fields and Buttons

Field/Button	Description
IP Address	Type the IP address of the ExtremeWireless Appliance's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Interface	From the drop-down list, select the physical port that provides the access to the VLAN.
VLAN ID	Type the VLAN tag to which the ExtremeWireless Appliance will be bridged for the VNS.
NAS	From the drop-down list, click the interface/port through which the NAC gateway will communicate with the ExtremeWireless Appliance. The IP address in this field will be used as the NAS IP RADIUS attribute when communicating with the NAC gateway.
NAC Server	
Server Alias	Type the name or IP address of the NAC server.
Hostname/IP	Type the NAC server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the ExtremeWireless Appliance and the NAC server. To proofread your shared secret key, click Unmask . The password is displayed. Note: You should always proofread your Shared Secret key to avoid any problems later when the wireless appliance attempts to communicate with the NAC controller.
NAC web server IP	Type the NAC web server IP address.

- 5 To save your changes, click **Finish**.

The VNS wizard creates a SSID-based NAC controller-compatible VNS, and displays the configuration summary.

- 6 To close the VNS wizard, click **Close**.

If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Voice VNS Using the VNS Wizard

Use the VNS wizard to create a voice-specific VNS that can support various wireless telephones, including optiPoint, Spectralink, Vocera, and Mobile Connect - Nokia.

When you use the VNS wizard to create a voice-specific VNS, you optimize the voice VNS to support one wireless telephone vendor. If the voice VNS needs to be optimized for more than one wireless phone vendor, use the advanced method to create the voice-specific VNS. For more information, see [Enabling and Disabling a VNS](#) on page 437.

When you create a new voice VNS using the VNS wizard, you configure the VNS in the following stages:

- [Basic settings](#)
- [Authentication settings](#), if applicable
- [DHCP settings](#)
- [Privacy settings](#)
- [Radio assignment settings](#)
- [Summary](#)

To configure a Voice VNS using the VNS Wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the New pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen displays.

VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

Name:

Category:

(Next: Basic Settings)

Back Next Cancel

- 3 In the **Name** box, type a name for the voice VNS.
- 4 In the **Category** drop-down list, click **Voice**.
- 5 Click **Next**. The [Basic Settings](#) screen displays.

Creating a Voice VNS Using the VNS Wizard - Basic Settings Screen

The **Basic Settings** screen displays:

Basic Settings
Test, Voice

Enabled:

Name: Test

Category: Voice

SSID: Test

Type: -

Mode: -

(Next: Privacy) Back Next Cancel

Table 66: Voice VNS Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	By default, the Synchronize checkbox for the new VNS is disabled.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Type	Click the wireless phone you want to support for the new voice VNS you are creating.
Mode	Click the VNS Mode you want to assign: <ul style="list-style-type: none"> • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type that has associated with it a Topology with a mode of Bridge Traffic Locally at EWC. User traffic is tunneled to the controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.
Routed Voice VNS	

Table 66: Voice VNS Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Type the controller's own IP address of the topology associated with that VNS. This IP address is also the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Gateway/SVP	If the voice VNS is to support Spectralink wireless phones, type the IP address of the SpectraLink Voice Protocol (SVP) gateway.
Vocera Server	If the voice VNS is to support Vocera wireless phones, type the IP address of the Vocera server.
PBX Server	If the voice VNS is to support either WL2 or Mobile Connect - Nokia wireless phones, type the PBX IP address.
Enable Authentication	If applicable, select this checkbox to enable authentication for the new voice VNS.
Enable	By default, this option is selected.
Bridge Traffic Locally- Voice VNS	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
Gateway/SVP	If the voice VNS is to support Spectralink wireless phones, type the IP address of the SpectraLink Voice Protocol (SVP) gateway.
Vocera Server	If the voice VNS is to support Vocera wireless phones, type the IP address of the Vocera server.
PBX Server	If the voice VNS is to support either WL2 or Mobile Connect - Nokia wireless phones, type the PBX IP address.
Enable Authentication	If applicable, select this checkbox to enable authentication for the new voice VNS.
Enable DHCP	If applicable, select this checkbox to enable DHCP authentication for the new voice VNS.

Click **Next**. The **Authentication** screen displays.

Creating a Voice VNS Using the VNS Wizard - Authentication Settings Screen

The **Authentication** screen displays:

Table 67: Voice VNS Authorization Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new voice VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: <ul style="list-style-type: none"> • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the voice VNS. • If applicable, and the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam.
Radius Server	Click the RADIUS server you want to assign to the new data VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.

Click **Next**. The **DHCP** screen displays.

Creating a Voice VNS Using the VNS Wizard - DHCP Screen

The **DHCP** screen displays:

Table 68: Voice VNS DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	<p>From the drop-down list, click one of the following:</p> <ul style="list-style-type: none"> • Use DHCP Relay — Using relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — Type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. <p>The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)</p> <ul style="list-style-type: none"> • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Servers	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Privacy** screen displays.

Creating a Voice VNS Using the VNS Wizard - Privacy Screen

The **Privacy** screen displays:

- 1 Most options on this screen are view-only, but you can do the following:
 - **Pre-shared key** — Type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key.
 - **Mask/Unmask** — Click to display or hide your shared secret key.
- 2 Click **Next**. The **Radio Assignment** screen displays.

Creating a Voice VNS Using the VNS Wizard - Radio Assignment Screen

The **Radio Assignment** screen displays:

Radio Assignment
Test, Voice, SpectraLink

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

Radio 1
 Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:

WMM:

WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary)

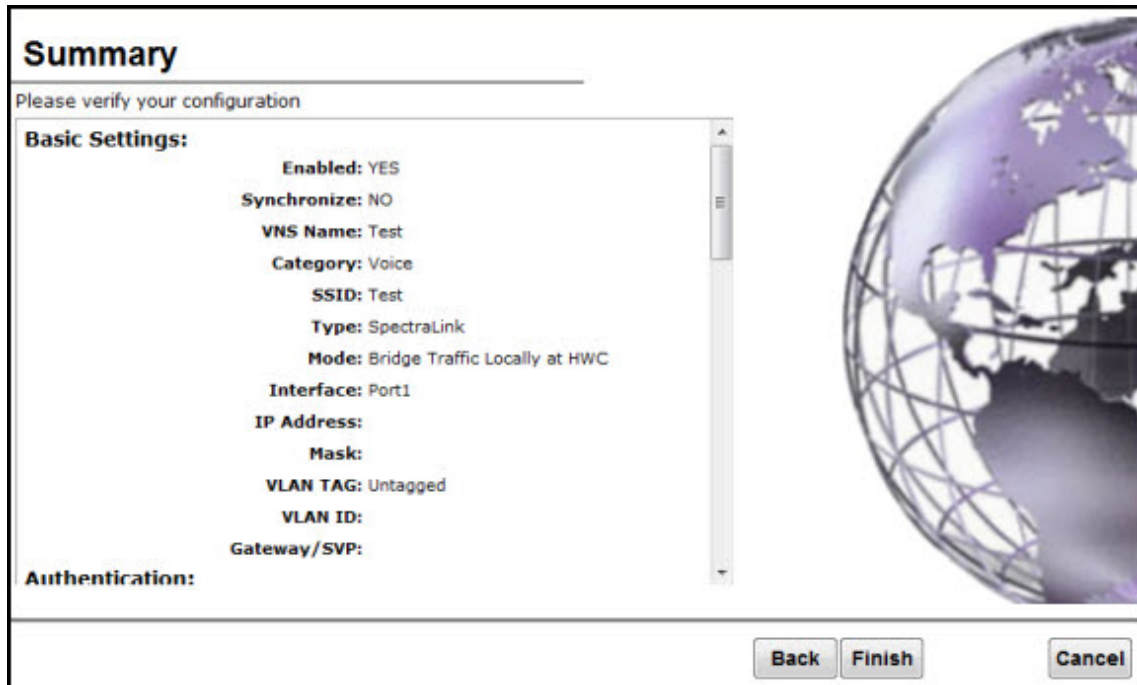
Table 69: Voice VNS Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the voice VNS.
AP Selection	
Select APs	Select the group of APs that will broadcast the voice VNS: <ul style="list-style-type: none"> • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the out traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating a Voice VNS Using the VNS Wizard - Summary Screen

The **Summary** screen displays:



- 1 Confirm your voice VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Data VNS Using the VNS Wizard

Use the VNS wizard to create a data-specific VNS that can be configured to use either SSID or AAA authentication.

When you create a new data VNS using the VNS wizard, you configure the VNS in the following stages:

- [Basic settings](#)
- [Authentication settings](#)
- [DHCP settings](#)
- [Filter settings](#)
- [Privacy settings](#)
- [Radio assignment settings](#)
- [Summary](#)

To configure a data VNS using the VNS wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- In the left pane, expand the New pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen displays.

VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

Name:

Category:

(Next: Basic Settings)

- In the **Name** box, type a name for the data VNS.
- In the **Category** drop-down list, click **Data**.
- Click **Next**. The **Basic Settings** screen displays.

Creating a Data VNS Using the VNS Wizard - Basic Settings Screen

The **Basic Settings** screen displays:

 Synchronize: Name: Test Category: Data SSID: Test Authentication Mode: - Mode: -'. To the right is a globe graphic. At the bottom, there is a navigation bar with the text '(Next: Privacy)', a 'Back' button, a 'Next' button, and a 'Cancel' button."/>

Basic Settings
Test Data

Enabled: Synchronize:

Name: Test
Category: Data
SSID: Test
Authentication Mode:
Mode:

(Next: Privacy)

Table 70: Data VNS Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	By default, the Synchronize checkbox for the new VNS is disabled.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click the type of network assignment for the VNS. There are two options for network assignment, Disabled or 802.1x.
Mode	Click the VNS mode you want to assign: <ul style="list-style-type: none"> • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN. • Bridge Traffic Locally at AP is a VNS type where user traffic is directly bridged to a VLAN at the AP network point of access (switch port).
Routed Data VNS	
Gateway	Type the controller's own IP address of the topology associated with that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Enable Authentication	This option is enabled by default if the Type is 802.1x.
Enable	By default, this option is enabled for a routed data VNS.
Bridged Traffic Locally @ AP Data VNS	
Tagged	Select if you want to assign this VNS to a specific VLAN.
VLAN ID	Type the VLAN tag to which the controller will be bridged for the data VNS.
Untagged	Select if you want this VNS to be untagged. This option is selected by default.
Enable Authentication	If applicable, select this checkbox to enable authentication for the new data VNS. This option is enabled by default if the Type is 802.1x.

Table 70: Data VNS Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Bridge Traffic Locally at EWC Data VNS	
Interface	Click the physical port that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
Enable Authentication	If applicable, select this checkbox to enable authentication for the new data VNS. This option is enabled by default if the Type is 802.1x.
Enable DHCP	If applicable, select this checkbox to enable DHCP authentication for the new data VNS.

Click **Next**. The **Authentication** screen displays.

Creating a Data VNS Using the VNS Wizard - Authentication Screen

The **Authentication** screen displays:

Table 71: Data VNS Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new data VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: <ul style="list-style-type: none"> • MAC-based Authentication – Select to enable the RADIUS server to perform MAC-based authentication on the data VNS. • If applicable, and the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam.

Click **Next**. The **DHCP** screen displays.

Creating a Data VNS Using the VNS Wizard - DHCP Screen

If was enabled previously, the **DHCP** screen displays:

DHCP
Test, Data, 802.1x

DHCP Option: Local DHCP Server ▼

Address Range: From: 127.0.1.2
To: 127.0.1.254

B'cast Address: 127.0.1.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering)

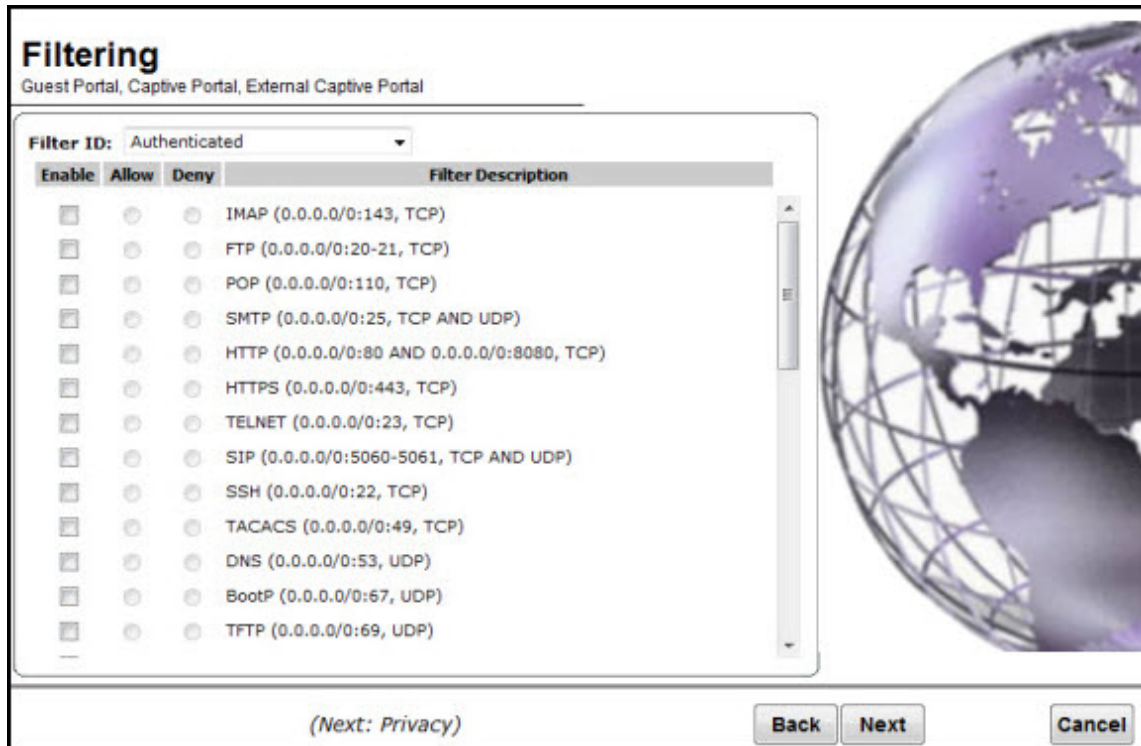
Table 72: Data VNS DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	<p>In the DHCP Option drop-down list, click one of the following:</p> <ul style="list-style-type: none"> • Use DHCP Relay — Using DHCP relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating a Data VNS Using the VNS Wizard - Filtering Screen

The **Filtering** screen displays:



- In the **Filter ID** drop-down list, click one of the following:
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters
- In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** checkbox accordingly.
- Click **Next**. The **Privacy** screen displays.

Creating a Data VNS Using the VNS Wizard - Privacy Screen

The **Privacy** screen displays:

Table 73: Data VNS Privacy Page - Fields and Buttons

Field/Button	Description
Static Keys (WEP)	<p>Select to configure static keys. Then enter:</p> <ul style="list-style-type: none"> • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. <p>Specifying the WEP key index is supported only for AP37XX wireless APs.</p> <ul style="list-style-type: none"> • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. <p>Select an Input Method:</p> <ul style="list-style-type: none"> • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
Dynamic Keys	Select to allow the dynamic key WEP mechanism to change the key for each user and each session.

Table 73: Data VNS Privacy Page - Fields and Buttons (continued)

Field/Button	Description
WPA	<p>Select to configure Wi-Fi Protected Access (WPA v1 and WPA v2), a security solution that adds authentication to enhanced WEP encryption and key management.</p> <p>To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. <p>To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard).
WPA-PSK	<p>AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.</p> <p>To enable re-keying after a time interval, select Broadcast re-key interval, then type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.</p> <p>If this checkbox is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.</p> <p>To enable the group key power save retry, select Group Key Power Save Retry.</p> <p>The group key power save retry is supported only for AP37XX wireless APs.</p> <p>In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key.</p> <p>Mask/Unmask — Click to display or hide your shared secret key.</p>

Click **Next**. The **Radio Assignment** screen displays.

Creating a Data VNS Using the VNS Wizard - Radio Assignment Screen

The **Radio Assignment** screen displays:

Radio Assignment
Test, Data, 802.1x

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

Radio 1
 Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:

WMM:

WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary)

Table 74: Data VNS Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the data VNS.
AP Selection	
Select APs	Select the group of APs that will broadcast the data VNS: <ul style="list-style-type: none"> • all radios – Click to assign all of the APs' radios. • radio 1 – Click to assign only the APs' Radio 1. • radio 2 – Click to assign only the APs' Radio 2. • local APs - all radios – Click to assign only the local APs. • local APs - radio 1 – Click to assign only the local APs' Radio 1. • local APs - radio 2 – Click to assign only the local APs' Radio 2. • foreign APs - all radios – Click to assign only the foreign APs. • foreign APs - radio 1 – Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 – Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating a Data VNS Using the VNS Wizard - Summary Screen

The **Summary** screen displays:

Summary

Please verify your configuration

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: Test
- Category: Data
- SSID: Test
- Type: 802.1x
- Mode: Routed
- Gateway:
- Mask:

Authentication:

- Server Alias: 10_109_0_6
- Roles:
- Authentication: YES
- MAC-based Authentication: YES

Buttons: Back, Finish, Cancel

- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
The data VNS is created and saved.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.
If the controller is configured to be part of an availability pair, you can choose to synchronize the VNS on the secondary controller. See [Availability and Session Availability](#) on page 490 for more information.

Creating a Captive Portal VNS Using the VNS Wizard

Use the VNS wizard to create a Captive Portal VNS. A Captive Portal VNS employs an authentication method that uses a Web redirection which directs a mobile user's Web session to an authentication server. Typically, the mobile user must provide their credentials (user ID, password) to be authenticated. You can create the following types of Captive Portal VNSs:

- **Internal Captive Portal** — The controller's own Captive Portal authentication page — configured as an editable form — is used to request user credentials. The redirection triggers the locally stored authentication page where the mobile user must provide the appropriate credentials, which then is checked against what is listed in the configured RADIUS server.
- **External Captive Portal** — An entity outside of the controller is responsible for handling the mobile user authentication process, presenting the credentials request forms and performing user authentication procedures. The external Web server location must be explicitly listed as an allowed destination in the non-authenticated filter.
- **Firewall Friendly External Captive Portal** — A Firewall Friendly External Captive Portal VNS provides wireless connections to any device on the secure side (behind the Firewall). When you create a new captive portal VNS using the VNS wizard, you configure the VNS in the following stages:

- **GuestPortal** — A GuestPortal VNS provides wireless device users with temporary guest network services.
- Basic settings
- Authentication settings
- settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary review

Related Links

[Creating an Internal Captive Portal VNS](#) on page 397

[Creating an External Captive Portal VNS](#) on page 406

[Creating a Firewall Friendly External Captive Portal VNS](#) on page 418

[Creating a GuestPortal VNS](#) on page 429

Creating an Internal Captive Portal VNS

To configure an Internal Captive Portal VNS using the VNS Wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the New pane, then click **START VNS WIZARD**. The **vns Creation Wizard** screen displays.

- 3 In the **Name** box, type a name for the Captive Portal VNS.
- 4 In the **Category** drop-down list, click **Captive Portal**.
- 5 Click **Next**. The **Basic Settings** screen displays.

Creating an Internal Captive Portal VNS - Basic Settings Screen

The **Basic Settings** screen displays:

Basic Settings
Captive Portal 000, Captive Portal

Enabled:
 Synchronize:
 Name: Captive Portal 000
 Category: Captive Portal
 SSID: Captive Portal 000
 Authentication Mode: -
 Mode: -

(Next: Privacy) Back Next Cancel

Table 75: Captive Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click Internal Captive Portal
Mode	Click the VNS Mode you want to assign: Routed is a VNS type where user traffic is tunneled to the controller. Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.
	Routed Internal Captive Portal

Table 75: Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Message	Type a brief message that will be displayed above the Login button that greets the mobile device user.
Enable Authentication	By default, this option is selected if the VNS Type is Internal Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	By default, this option is selected if the VNS Type is Internal Captive Portal , which enables authentication for the new Captive Portal VNS.
Bridge Traffic Locally- Voice VNS	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
Message	Type a brief message that will be displayed above the Login button that greets the mobile device user.
Enable Authentication	By default, this option is selected if the VNS Type is Internal Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	If applicable, select this checkbox to enable DHCP authentication for the new Captive Portal VNS.

Click **Next**. The **Authentication** screen displays

Creating an Internal Captive Portal VNS - Authentication Screen

The **Authentication** screen displays:

Table 76: Captive Portal Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new Captive Portal VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: <ul style="list-style-type: none"> • Authentication — By default, this option is selected if the VNS Type is Internal Captive Portal, which enables the RADIUS server to perform authentication on the Captive Portal VNS. • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS. If the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam, if applicable. • Accounting — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.

Click **Next**. The **DHCP** screen displays.

Creating an Internal Captive Portal VNS - DHCP Screen

The **DHCP** screen displays:

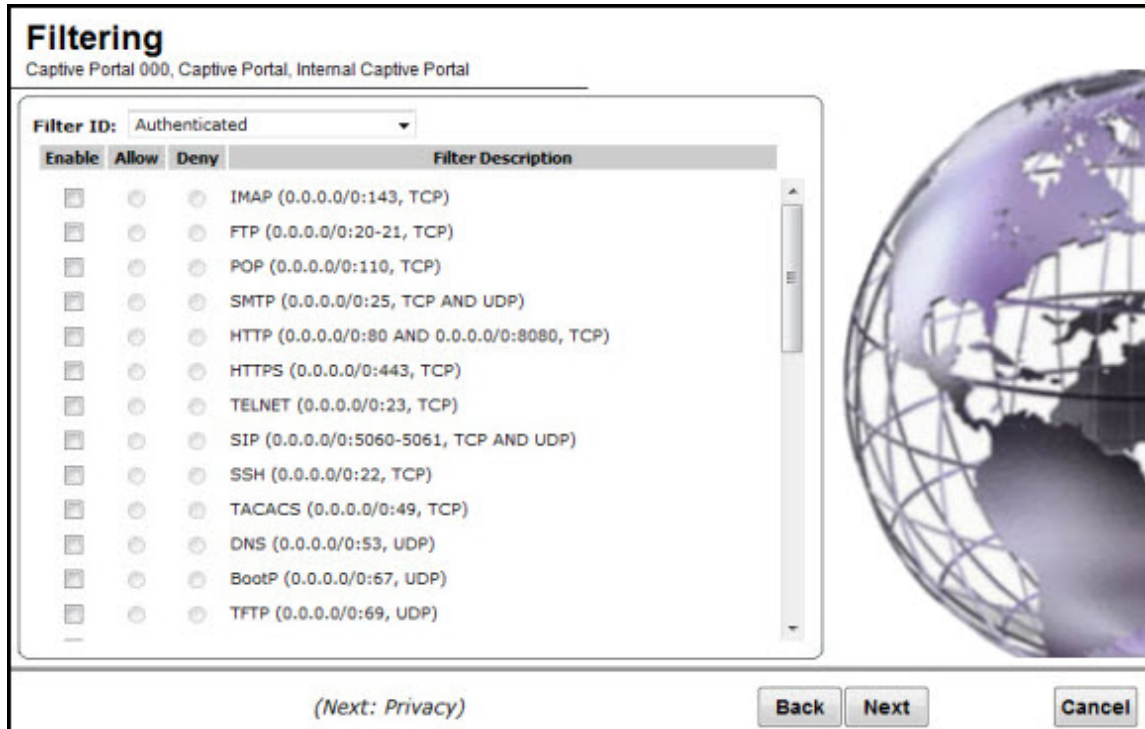
Table 77: Captive Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	<p>In the DHCP Option drop-down list, click one of the following:</p> <ul style="list-style-type: none"> • Use DHCP Relay — Using relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating an Internal Captive Portal VNS - Filtering Screen

The **Filtering** screen displays:



- 1 In the **Filter ID** drop-down list, click one of the following:
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the ExtremeWireless Controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
 - **Non-Authenticated** — Controls network access and also used to direct mobile users to a Captive Portal web page for login.
- 2 In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** checkbox accordingly.
- 3 Click **Next**.
The **Privacy** screen displays.

Creating an Internal Captive Portal VNS - Privacy Screen

The **Privacy** screen displays:

Privacy

Captive Portal 000, Captive Portal, Internal Captive Portal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

None

Static Keys (WEP)

WPA - PSK

(Next: RF)

Back **Next** **Cancel**




Table 78: Captive Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	<p>Select to configure static keys. Then enter:</p> <p>WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. Specifying the WEP key index is supported only for AP37XX wireless APs.</p> <p>WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit.</p> <p>Select an Input Method:</p> <p>Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input.</p> <p>Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.</p>
WPA-PSK	<p>Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.</p> <p>To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. <p>To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. <p>To enable re-keying after a time interval, select Broadcast re-key interval. If this checkbox is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.</p> <p>In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically.</p> <p>To enable the group key power save retry, select Group Key Power Save Retry.</p> <p>The group key power save retry is supported only for AP37XX wireless APs. In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key.</p> <p>Mask/Unmask — Click to display or hide your shared secret key.</p>

Click **Next**. The **Radio Assignment** screen displays

Creating an Internal Captive Portal VNS - Radio Assignment Screen

The **Radio Assignment** screen displays:

Radio Assignment
Captive Portal 000, Captive Portal, Internal Captive Portal

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

Radio 1
 Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:

WMM:

WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	0409920201201314
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary)

Table 79: Captive Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	
Select APs	Select the group of APs that will broadcast the Captive Portal VNS: <ul style="list-style-type: none"> • all radios – Click to assign all of the APs' radios. • radio 1 – Click to assign only the APs' Radio 1. • radio 2 – Click to assign only the APs' Radio 2. • local APs - all radios – Click to assign only the local APs. • local APs - radio 1 – Click to assign only the local APs' Radio 1. • local APs - radio 2 – Click to assign only the local APs' Radio 2. • foreign APs - all radios – Click to assign only the foreign APs. • foreign APs - radio 1 – Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 – Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays

Creating an Internal Captive Portal VNS - Summary Screen

The **Summary** screen displays:

Summary

Please verify your configuration

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: Captive Portal 000
- Category: Captive Portal
- SSID: Captive Portal 000
- Type: Internal Captive Portal
- Mode: Routed
- Gateway:
- Mask:

Authentication:

- Server Alias: 10_109_0_6
- Roles:
- Authentication: YES
- MAC-based Authentication: NO

Back Finish Cancel

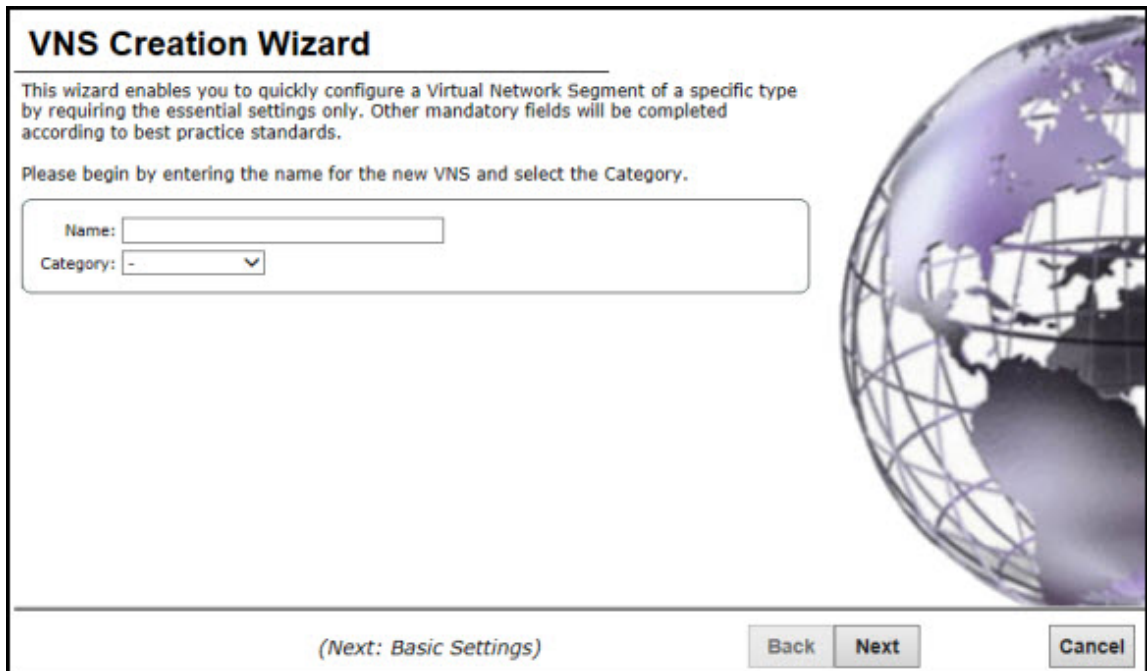
- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating an External Captive Portal VNS

To configure an external Captive Portal VNS using the VNS wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- In the left pane, expand the New pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen displays.



VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

Name:

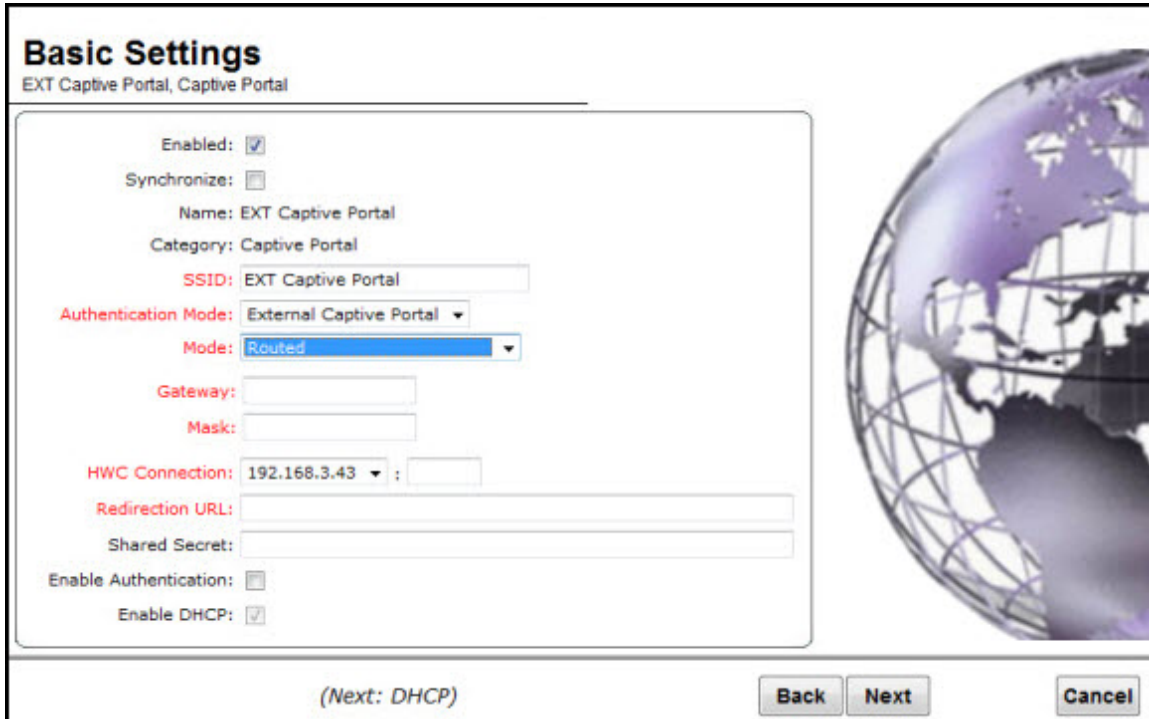
Category:

(Next: Basic Settings)

- In the **Name** box, type a name for the Captive Portal VNS.
- In the **Category** drop-down list, click **Captive Portal**.
- Click **Next**. The **Basic Settings** screen displays.

Creating an External Captive Portal VNS - Basic Settings Screen

The **Basic Settings** screen displays:



Basic Settings
EXT Captive Portal, Captive Portal

Enabled:
 Synchronize:
 Name: EXT Captive Portal
 Category: Captive Portal
 SSID: EXT Captive Portal
 Authentication Mode: External Captive Portal
 Mode: Routed
 Gateway:
 Mask:
 HWC Connection: 192.168.3.43 :
 Redirection URL:
 Shared Secret:
 Enable Authentication:
 Enable DHCP:

(Next: DHCP) Back Next Cancel

Table 80: External Captive Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	Synchronize — Enable automatic synchronization with its availability peer. Refer to Using the Sync Summary on page 365 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable this feature.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click External Captive Portal
Mode	Click the VNS Mode you want to assign: <ul style="list-style-type: none"> • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.

Table 80: External Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Routed External Captive Portal	
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
EWC Connection	Click the controller IP address. Also type the port of the controller in the accompanying box. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	By default, this option is selected if the VNS Type is External Captive Portal , which enables services for the new Captive Portal VNS.
EWC External Captive Portal VNS	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
EWC Connection	Click the controller IP address. Also type the port of the controller in the accompanying box. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.

Table 80: External Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	If applicable, select this checkbox to enable DHCP authentication for the new Captive Portal VNS.

Click **Next**. The **Authentication** screen displays.

Creating an External Captive Portal VNS - Authentication Screen

The VNS wizard displays the appropriate configuration screens, depending on your selection of the **Enable Authentication** and **Enable DHCP** checkboxes.

Table 81: External Captive Portal Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new Captive Portal VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.

Table 81: External Captive Portal Authentication Page - Fields and Buttons (continued)

Field/Button	Description
Mask/Unmask	Click to display or hide your shared secret key.
Roles	<p>Select the authentication role options for the RADIUS server:</p> <ul style="list-style-type: none"> • Authentication — By default, this option is selected if the VNS Type is External Captive Portal, which enables the RADIUS server to perform authentication on the Captive Portal VNS. • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS. If the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam, if applicable. • Accounting — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.

Click **Next**. The **DHCP** screen displays.

Creating an External Captive Portal VNS - DHCP Screen

The **DHCP** screen displays:

DHCP
EXT Captive Portal, Captive Portal, External Captive Portal

DHCP Option: Local DHCP Server ▾

Address Range: From: 127.0.1.2
To: 127.0.1.254

B'cast Address: 127.0.1.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering)

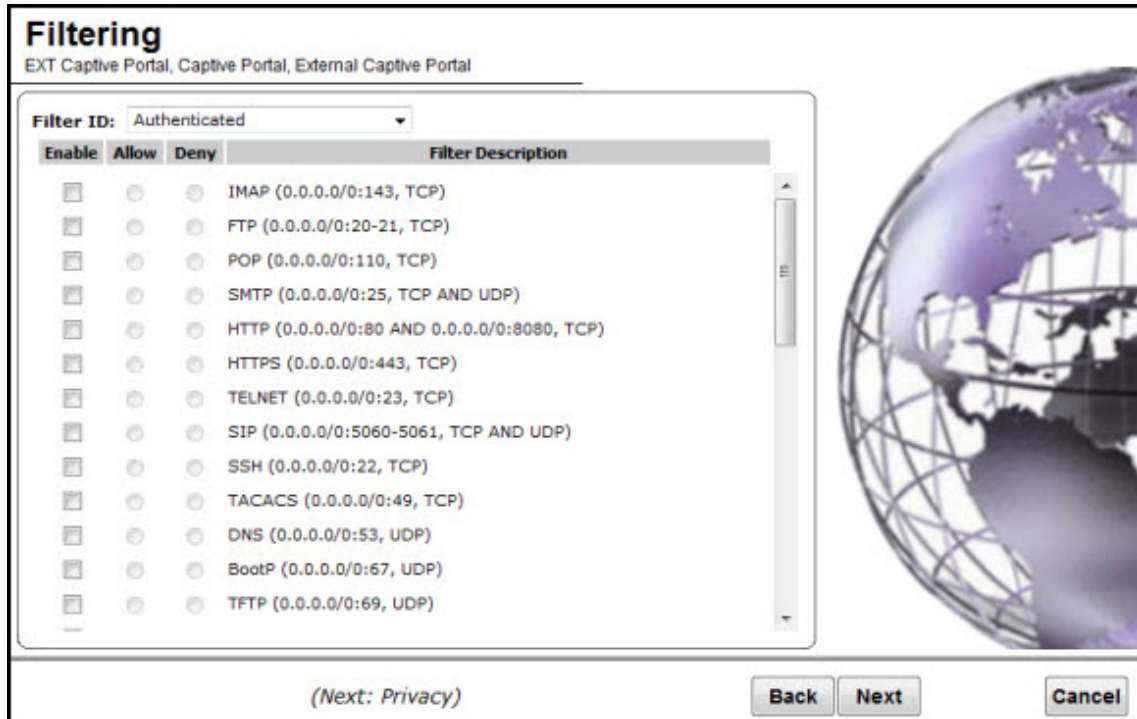
Table 82: External Captive Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	<p>In the DHCP Option drop-down list, click one of the following:</p> <ul style="list-style-type: none"> • Use DHCP Relay — Using relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating an External Captive Portal VNS - Filtering Screen

The **Filtering** screen displays:



- 1 In the **Filter ID** drop-down list, click one of the following:
 - **Default** – Controls access if there is no matching filter ID for a user.
 - **Exception** – Protects access to the controller’s own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the controller’s own interface point on the VNS. These filters are applied after the user’s specific VNS state assigned filters.
 - **Non-Authenticated** – Controls network access and also used to direct mobile users to a Captive Portal Web page for login.
- 2 In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** checkbox accordingly.
- 3 Click **Next**. The **Privacy** screen displays.

Creating an External Captive Portal VNS - Privacy Screen

The **Privacy** screen displays:

Privacy


EXT Captive Portal, Captive Portal, External Captive Portal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

None

Static Keys (WEP)

WPA - PSK



(Next: RF) Back Next Cancel

Table 83: External Captive Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	<p>Select to configure static keys. Then enter:</p> <ul style="list-style-type: none"> • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. <p>Specifying the WEP key index is supported only for AP37XX wireless APs.</p> <ul style="list-style-type: none"> • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. <p>Select an Input Method:</p> <ul style="list-style-type: none"> • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
WPA-PSK	<p>Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office. To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. <p>To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. <p>To enable re-keying after a time interval, select Broadcast re-key interval. If this checkbox is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications. In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically. To enable the group key power save retry, select Group Key Power Save Retry. The group key power save retry is supported only for AP37XX Wireless APs.</p>

Table 83: External Captive Portal Privacy Page - Fields and Buttons (continued)

Field/Button	Description
	In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. Mask/Unmask – Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating an External Captive Portal VNS - Radio Assignment Screen

The **Radio Assignment** screen displays:

Table 84: External Captive Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	

Table 84: External Captive Portal Radio Assignment Page - Fields and Buttons (continued)

Field/Button	Description
Select APs	Select the group of APs that will broadcast the Captive Portal VNS: <ul style="list-style-type: none"> • all radios – Click to assign all of the APs' radios. • radio 1 – Click to assign only the APs' Radio 1. • radio 2 – Click to assign only the APs' Radio 2. • local APs - all radios – Click to assign only the local APs. • local APs - radio 1 – Click to assign only the local APs' Radio 1. • local APs - radio 2 – Click to assign only the local APs' Radio 2. • foreign APs - all radios – Click to assign only the foreign APs. • foreign APs - radio 1 – Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 – Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating an External Captive Portal VNS - Summary Screen

The **Summary** screen displays:

Summary

Please verify your configuration

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: EXT Captive Portal
- Category: Captive Portal
- SSID: EXT Captive Portal
- Type: External Captive Portal
- Mode: Routed
- Gateway:
- Mask:
- HWC Connection: 192.168.3.43:
- Redirection URL:
- Shared Secret:

Authentication:

- Server Alias: 10_109_0_6

Back Finish Cancel

- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.

- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Firewall Friendly External Captive Portal VNS

To configure a Firewall Friendly External Captive Portal VNS using the VNS wizard:

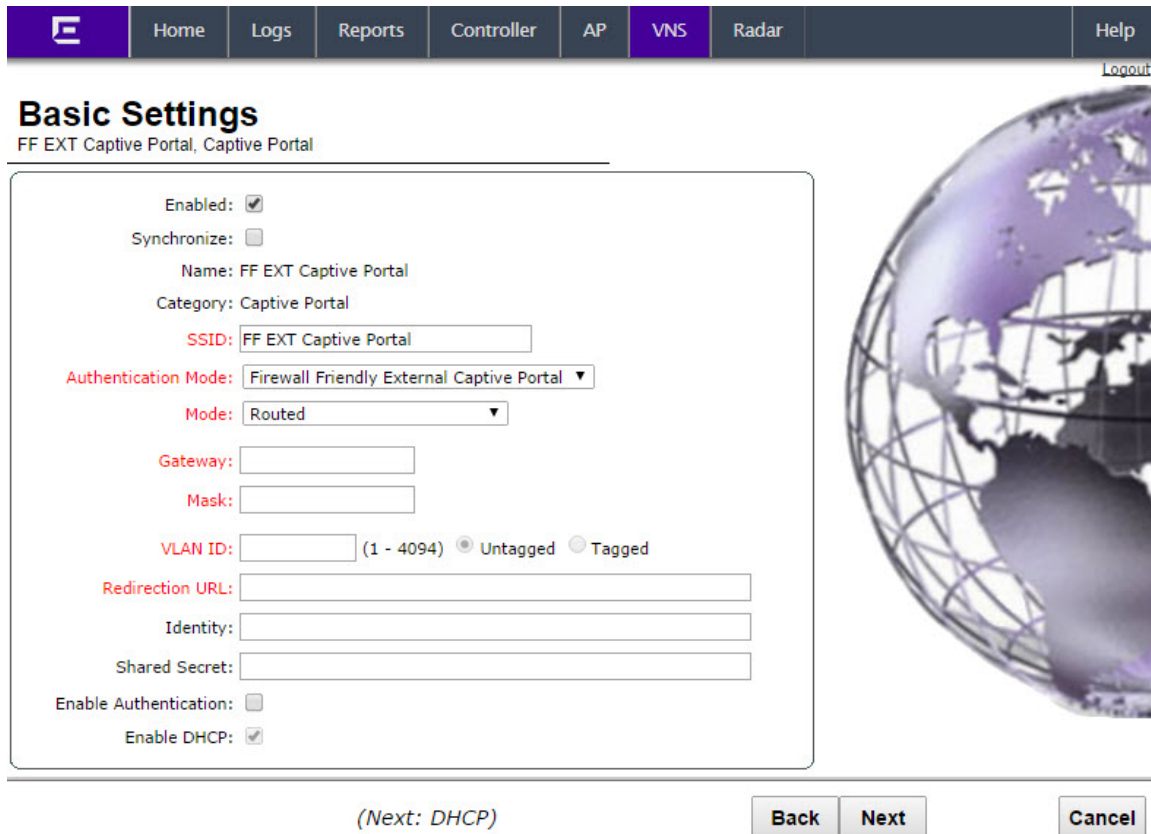
- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **New**, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen displays.

- 3 In the **Name** box, type a name for the Firewall Friendly Captive Portal VNS.
- 4 In the **Category** drop-down list, click **Captive Portal**.
- 5 Click **Next**. The **Basic Settings** screen displays.

If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Firewall Friendly External Captive Portal VNS - Basic Settings Screen

The **Basic Settings** screen displays:



Basic Settings
FF EXT Captive Portal, Captive Portal

Enabled:

Synchronize:

Name: FF EXT Captive Portal

Category: Captive Portal

SSID: FF EXT Captive Portal

Authentication Mode: Firewall Friendly External Captive Portal

Mode: Routed

Gateway:

Mask:

VLAN ID: (1 - 4094) Untagged Tagged

Redirection URL:

Identity:

Shared Secret:

Enable Authentication:

Enable DHCP:

(Next: DHCP)

Back Next Cancel

Table 85: Firewall Friendly External Captive Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click External Captive Portal
Mode	Click the VNS Mode you want to assign: <ul style="list-style-type: none"> Routed is a VNS type where user traffic is tunneled to the controller. Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.

Table 85: Firewall Friendly External Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	By default, this option is selected if the VNS Type is External Captive Portal , which enables services for the new Captive Portal VNS.
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
EWC Connection	Click the controller IP address. Also type the port of the controller in the accompanying box. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	If applicable, select this checkbox to enable DHCP authentication for the new Captive Portal VNS.

Click **Next**. The **Authentication** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Authentication Screen

The VNS wizard displays the appropriate configuration screens, depending on your selection of the **Enable Authentication** and **Enable DHCP** check boxes.

Table 86: Firewall Friendly External Captive Portal Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new Captive Portal VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: <ul style="list-style-type: none"> • Authentication — By default, this option is selected if the VNS Type is External Captive Portal, which enables the RADIUS server to perform authentication on the Captive Portal VNS. • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS. If the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam, if applicable. • Accounting — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.

Click **Next**. The **DHCP** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - DHCP Screen

The **DHCP** screen displays:

DHCP
FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

DHCP Option: Local DHCP Server ▼

Address Range: From: 192.168.101.1
To: 192.168.101.254

B'cast Address: 192.168.101.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering) **Back** **Next** **Cancel**

Table 87: External Captive Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	<p>In the DHCP Option drop-down list, click one of the following:</p> <ul style="list-style-type: none"> • Use DHCP Relay — Using relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Filtering Screen

The **Filtering** screen displays:

Filtering
FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

Filter ID:

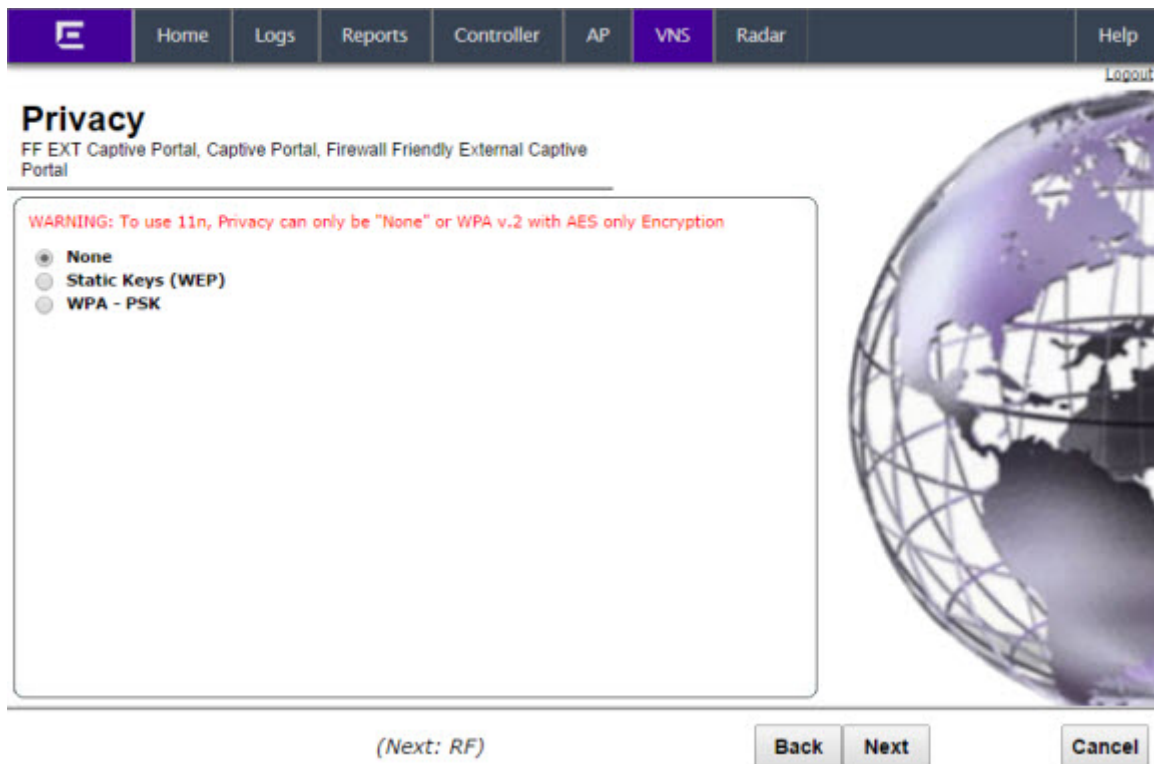
Enable	Allow	Deny	Filter Description
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	IMAP (0.0.0.0/0:143, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	FTP (0.0.0.0/0:20-21, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	POP (0.0.0.0/0:110, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SMTP (0.0.0.0/0:25, TCP AND UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	HTTP (0.0.0.0/0:80 AND 0.0.0.0/0:8080, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	HTTPS (0.0.0.0/0:443, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TELNET (0.0.0.0/0:23, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SIP (0.0.0.0/0:5060-5061, TCP AND UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SSH (0.0.0.0/0:22, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TACACS (0.0.0.0/0:49, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	DNS (0.0.0.0/0:53, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TFTP (0.0.0.0/0:69, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	Finger (0.0.0.0/0:79, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	Portmapper (0.0.0.0/0:111, UDP)

(Next: Privacy)

- In the **Filter ID** drop-down list, click one of the following:
 - Default** — Controls access if there is no matching filter ID for a user.
 - Exception** — Protects access to the controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
 - Non-Authenticated** — Controls network access and also used to direct mobile users to a Captive Portal Web page for login.
- In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** checkbox accordingly.
- Click **Next**. The **Privacy** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Privacy Screen

The **Privacy** screen displays:



The screenshot shows a web-based configuration interface for a VNS. At the top, there is a navigation bar with tabs for Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A Logout link is visible in the top right corner. The main heading is "Privacy", with subtext "FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal". A warning message in red text states: "WARNING: To use 11n, Privacy can only be 'None' or WPA v.2 with AES only Encryption". Below the warning, there are three radio button options: "None" (selected), "Static Keys (WEP)", and "WPA - PSK". To the right of the configuration area is a decorative image of a globe. At the bottom, there are three buttons: "Back", "Next", and "Cancel". A note "(Next: RF)" is positioned below the configuration area.

Home Logs Reports Controller AP **VNS** Radar Help Logout

Privacy

FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

- None
- Static Keys (WEP)
- WPA - PSK

(Next: RF) Back Next Cancel

Table 88: External Captive Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	<p>Select to configure static keys. Then enter:</p> <ul style="list-style-type: none"> • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. <p>Specifying the WEP key index is supported only for AP37XX wireless APs.</p> <ul style="list-style-type: none"> • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. <p>Select an Input Method:</p> <ul style="list-style-type: none"> • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
WPA-PSK	<p>Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.</p> <p>To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. <p>To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. <p>To enable re-keying after a time interval, select Broadcast re-key interval. If this checkbox is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.</p> <p>In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically.</p> <p>To enable the group key power save retry, select Group Key Power Save Retry.</p> <p>The group key power save retry is supported only for AP37XX wireless APs. In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key.</p>

Table 88: External Captive Portal Privacy Page - Fields and Buttons (continued)

Field/Button	Description
	Mask/Unmask – Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Radio Assignment Screen

The **Radio Assignment** screen displays:

Radio Assignment
FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

Radio 1
 Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:

WMM:
WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	AP2660 Dummy
a/n	b/g	AP3660 Dummy
a/n	b/g	AP3705i Dummy
a/n	b/g	AP3715e Dummy
a/n	b/g	AP3715i Dummy
a/n	b/g	AP3765e[F]
a/n	b/g	AP3765i Dummy
a/n/ac	b/g/n	ap3805_t
a/n/ac	b/g/n	AP3825i Dummy

(Next: Summary)

Table 89: External Captive Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	

Table 89: External Captive Portal Radio Assignment Page - Fields and Buttons (continued)

Field/Button	Description
Select APs	Select the group of APs that will broadcast the Captive Portal VNS: <ul style="list-style-type: none"> • all radios – Click to assign all of the APs' radios. • radio 1 – Click to assign only the APs' Radio 1. • radio 2 – Click to assign only the APs' Radio 2. • local APs - all radios – Click to assign only the local APs. • local APs - radio 1 – Click to assign only the local APs' Radio 1. • local APs - radio 2 – Click to assign only the local APs' Radio 2. • foreign APs - all radios – Click to assign only the foreign APs. • foreign APs - radio 1 – Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 – Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Summary Screen

The **Summary** screen displays:

The screenshot shows the Summary screen in a web interface. The navigation bar at the top includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A Logout link is visible in the top right corner. The main heading is "Summary" with a sub-heading "Please verify your configuration". The configuration details are displayed in a scrollable box:

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: FF EXT Captive Portal
- Category: Captive Portal
- SSID: FF EXT Captive Portal
- Type: Firewall Friendly External Captive Portal
- Mode: Routed
- Gateway: 192.168.101.2
- Mask: 255.255.255.0
- VLAN TAG: Untagged
- VLAN ID: 4094

Authentication:

- Radius Server: Add New Server
- Server Alias: test

At the bottom right of the screen, there are three buttons: Back, Finish, and Cancel. A globe graphic is visible on the right side of the screen.

- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.

Creating a GuestPortal VNS

A GuestPortal provides wireless device users with temporary guest network services. A GuestPortal is serviced by a GuestPortal-dedicated VNS. A controller is allowed only one GuestPortal-dedicated VNS at a time. GuestPortal user accounts are administered by a GuestPortal manager. A GuestPortal manager is a login group — GuestPortal managers must have their accounts created for them on the controller. For more information, see [Working with GuestPortal Administration](#) on page 635

The GuestPortal VNS is a Captive Portal authentication-based VNS that uses a database on the controller for managing user accounts. The database is administered through a simple, user-friendly graphic user interface that can be used by non-technical staff.

The GuestPortal VNS can be a Routed or a Bridge Traffic Locally at the EWC VNS, with SSID-based network assignment. The GuestPortal VNS is a simplified VNS. It does not support the following:

- RADIUS authentication or accounting
- MAC-based authorization
- Child VNS support

The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS. When you create a new VNS using the VNS wizard, you configure the VNS in the following stages:

- Basic settings
- settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary

Use the following high-level description to set up a GuestPortal on your system:

- 1 Create a GuestPortal VNS.
The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS.
- 2 Configure the GuestPortal ticket.
A GuestPortal account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account. For more information, see [Working with the Guest Portal Ticket Page](#) on page 645.
- 3 Configure availability, if applicable.
Availability maintains service availability in the event of a controller outage. For more information, see [Availability and Session Availability](#) on page 490.
- 4 Create GuestPortal manager and user accounts.
For more information, see [Working with GuestPortal Administration](#) on page 635
- 5 Manage your guest accounts and GuestPortal logs.
For more information, see the Extreme Networks ExtremeWireless *Maintenance Guide*.

Creating a GuestPortal VNS from an Existing VNS

The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS. A controller is allowed only one GuestPortal-dedicated VNS at a time.

To create a GuestPortal VNS from an already existing VNS:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, select and expand the **Virtual Networks** pane.
- 3 Click on the VNS you want to configure as a GuestPortal VNS. The VNS configuration window **Core** tab is displayed.
- 4 Select a preconfigured WLAN Service and click **Edit**, or press **New** to create a new WLAN Service.
- 5 In the Edit WLAN Service window, click the **Auth & Acct** tab
- 6 In the **Authentication Mode** drop-down list, click **GuestPortal**.
- 7 To save your changes, click **Save**.

Creating a New GuestPortal VNS Using the VNS Wizard

To create a new GuestPortal VNS using the VNS Wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the **New** pane, and then click **START VNS WIZARD**. The **VNS Creation Wizard** screen displays.

- 3 In the **Name** box, type a name for the GuestPortal VNS.
- 4 In the **Category** drop-down list, click **Captive Portal**.
- 5 Click **Next**. The **Basic Settings** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Basic Settings Screen

The **Basic Settings** screen displays:

Basic Settings
Guest-Portal, Captive Portal

Enabled:

Synchronize:

Name: Guest-Portal

Category: Captive Portal

SSID:

Authentication Mode:

Mode:

Gateway:

Mask:

Enable DHCP:

(Next: DHCP)

Back Next Cancel

Table 90: Guest Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled checkbox for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	By default, the Synchronize checkbox for the new VNS is disabled.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click Guest Portal
Mode	Click the VNS Mode you want to assign: <ul style="list-style-type: none"> • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific VLAN. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.
Routed	

Table 90: Guest Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Bridge Traffic Locally at EWC	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN to which the controller will be bridged for the VNS. Then, select either Untagged or Tagged .
Enable DHCP	If applicable, select this checkbox to enable .

Click **Next**. The **DHCP** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - DHCP Screen

The **DHCP** screen displays:

DHCP
Guest Portal, Captive Portal, External Captive Portal

DHCP Option: Local DHCP Server ▾

Address Range: From: 127.0.1.2
To: 127.0.1.254

B'cast Address: 127.0.1.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering)

Table 91: Guest Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	<p>In the DHCP Option drop-down list, click one of the following:</p> <p>Use DHCP Relay — Using relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.</p> <p>DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)</p> <p>Local DHCP Server — If applicable, edit the local DHCP server settings.</p>
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Filtering Screen

The **Filtering** screen displays:

Filtering
Guest Portal, Captive Portal, External Captive Portal

Filter ID: Authenticated

Enable	Allow	Deny	Filter Description
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	IMAP (0.0.0.0/0:143, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	FTP (0.0.0.0/0:20-21, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	POP (0.0.0.0/0:110, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SMTP (0.0.0.0/0:25, TCP AND UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	HTTP (0.0.0.0/0:80 AND 0.0.0.0/0:8080, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	HTTPS (0.0.0.0/0:443, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TELNET (0.0.0.0/0:23, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SIP (0.0.0.0/0:5060-5061, TCP AND UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SSH (0.0.0.0/0:22, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TACACS (0.0.0.0/0:49, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	DNS (0.0.0.0/0:53, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	BootP (0.0.0.0/0:67, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	TFTP (0.0.0.0/0:69, UDP)

(Next: Privacy)

Back Next Cancel

- 1 Configure the VNS filtering settings:
 - a In the **Filter ID** drop-down list, click one of the following:
 - **Authenticated** — Controls network access after the user has been authenticated.
 - **Non-authenticated** — Controls network access and to direct users to a Captive Portal Web page for login.
- 2 In the **Filter** table, select the **Enable** checkbox for the desired filters, then select the **Allow** or **Deny** option buttons for each filter as needed.
- 3 At the bottom of the Filter list, select **Allow** or **Deny** for **All Other Traffic**.
- 4 Click **Next**. The **Privacy** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Radio Assignment Screen

The **Radio Assignment** screen displays:

Radio Assignment
Guest-Portal, Captive Portal, GuestPortal

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

Radio 1
 Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs: -
WMM:
WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	0409920201201314
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary) Back Next Cancel

Table 92: Guest Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	

Table 92: Guest Portal Radio Assignment Page - Fields and Buttons (continued)

Field/Button	Description
Select APs	Select the group of APs that will broadcast the Captive Portal VNS: <ul style="list-style-type: none"> • all radios – Click to assign all of the APs' radios. • radio 1 – Click to assign only the APs' Radio 1. • radio 2 – Click to assign only the APs' Radio 2. • local APs - all radios – Click to assign only the local APs. • local APs - radio 1 – Click to assign only the local APs' Radio 1. • local APs - radio 2 – Click to assign only the local APs' Radio 2. • foreign APs - all radios – Click to assign only the foreign APs. • foreign APs - radio 1 – Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 – Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Privacy Screen

The **Privacy** screen displays:

Privacy
Guest Portal, Captive Portal, GuestPortal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

None
 Static Keys (WEP)
 WPA - PSK

WPA v.1
Encryption: Auto

WPA v.2
Encryption: Auto

Broadcast re-key interval: 3600 seconds (30 - 86400 seconds)

Input Method: Input String Input Hex

Pre-shared key String: Unmask
(min 8 characters; max 63)

(Next: RF) Back Next Cancel

Table 93: Guest Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	<p>Select to configure static keys. Then enter:</p> <ul style="list-style-type: none"> • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. <p>Specifying the WEP key index is supported only for AP37XX wireless APs.</p> <ul style="list-style-type: none"> • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. <p>Select an Input Method:</p> <ul style="list-style-type: none"> • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
WPA-PSK	<p>Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office. To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. <p>To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types:</p> <ul style="list-style-type: none"> • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. <p>To enable re-keying after a time interval, select Broadcast re-key interval. If this checkbox is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications. In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically. To enable the group key power save retry, select Group Key Power Save Retry. The group key power save retry is supported only for AP37XX wireless APs.</p>

Table 93: Guest Portal Privacy Page - Fields and Buttons (continued)

Field/Button	Description
	In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. Mask/Unmask – Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Summary Screen

The **Summary** screen displays:

Summary

Please verify your configuration

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: Guest-Portal
- Category: Captive Portal
- SSID: Guest-Portal
- Type: GuestPortal
- Mode: Routed
- Gateway:
- Mask:

DHCP:

- DHCP Option: Local DHCP Server
- Address Range:
 - From: 127.0.1.2
 - To: 127.0.1.254

Buttons: Back, Finish, Cancel

- 1 Confirm your VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
If the controller is configured to be part of an availability pair, you can choose to synchronize the VNS on the secondary controller.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Enabling and Disabling a VNS

By default, when a new VNS is created, the VNS is added to the system as an enabled VNS. A VNS can be enabled or disabled. Disabling a VNS provides the ability to temporarily stop wireless service on a VNS. The disabled VNS configuration remains in the database for future use.

The controller can support the following VNSs:

Table 94: ExtremeWireless Appliance Active and Defined VNS Support

Platform	Active VNSs	Defined VNSs
C5110	128	256
C5210	128	256
C4110	64	128
C25	16	32
C35	16	32
V2110 (Small)	16	32
V2110 (Medium)	64	128
V2110 (Large)	128	256

To enable or disable a VNS:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **Virtual Networks** pane and select the VNS to enable or disable.
- 3 On the **Core** tab, in the Status box, select or de-select the **Enable** checkbox.
- 4 Click **Save**. The VNS is enabled or disabled accordingly.

Renaming a VNS

To rename a VNS:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **Virtual Networks** pane, then select the VNS you want to rename.
- 3 On the **Core** tab, in the **VNS Name** field, enter the new name.
- 4 Click **Save**. The VNS is renamed.

Deleting a VNS

You can delete a VNS that is no longer necessary.

To delete a VNS:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **Virtual Networks** pane, then select the VNS you want to rename.
- 3 On the **Core** tab, click the **Delete** button. A pop-up window prompts you to confirm you want to delete the VNS. Click **OK**.
- 4 Click **Save**. The VNS is deleted.

9 Configuring Classes of Service

Classes of Service Overview
Configuring Classes of Service
CoS Rule Classification
Priority and ToS/DSCP Marking
Rate Limiting

Classes of Service Overview

In general, 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. For more information on configuring roles, see [Configuring Default VLAN and Class of Service for a Role](#) on page 240.

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.
- Transmit queue assignment

The system limit for the number of CoS profiles on a controller is identical to the number of roles. For example, a C5110 can have 1024 roles and 1024 CoS profiles.

Configuring Classes of Service

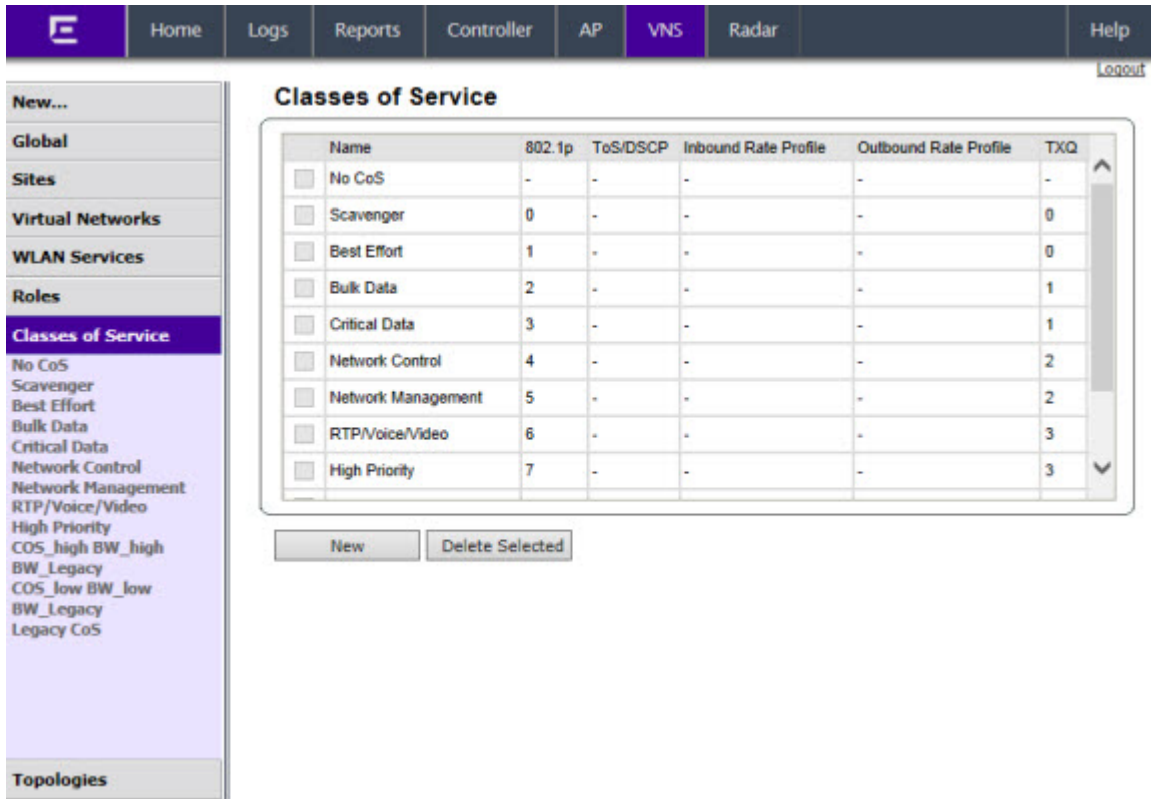
The feature is a configuration entity containing QoS Marking (802.1p and ToS/DSCP), Inbound/Outbound Rate Limiting and Transmit Queue Assignments. The CoS ToS marking capability allows for NAC-based redirection to different captive portals on the same WLAN Service.

The supported CoS attributes are enforced on the controller (data plane) and on the APs.

To configure Classes of Service:

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

- 2 In the left pane click **Classes of Service**.



The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. The left sidebar contains a navigation menu with categories: New..., Global, Sites, Virtual Networks, WLAN Services, Roles, and Topologies. Under Roles, 'Classes of Service' is selected, showing a list of predefined classes: No CoS, Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, RTP/Voice/Video, High Priority, COS_high BW_high, BW_Legacy, COS_low BW_low, BW_Legacy, and Legacy CoS. The main content area displays a table titled 'Classes of Service' with columns: Name, 802.1p, ToS/DSCP, Inbound Rate Profile, Outbound Rate Profile, and TXQ. Below the table are 'New' and 'Delete Selected' buttons.

Name	802.1p	ToS/DSCP	Inbound Rate Profile	Outbound Rate Profile	TXQ
<input type="checkbox"/> No CoS	-	-	-	-	-
<input type="checkbox"/> Scavenger	0	-	-	-	0
<input type="checkbox"/> Best Effort	1	-	-	-	0
<input type="checkbox"/> Bulk Data	2	-	-	-	1
<input type="checkbox"/> Critical Data	3	-	-	-	1
<input type="checkbox"/> Network Control	4	-	-	-	2
<input type="checkbox"/> Network Management	5	-	-	-	2
<input type="checkbox"/> RTP/Voice/Video	6	-	-	-	3
<input type="checkbox"/> High Priority	7	-	-	-	3

Note



"No CoS" means that the traffic to which it is assigned will not be remarked, the controller software will decide the appropriate transmit queue and no rate limits will be applied on traffic traveling to or from the station to which the CoS is applied. The "No CoS" CoS is predefined and cannot be removed.

- In the left pane, click the name of the Classes of Service that you want to edit, or click the **New** button to create a new CoS. The **Class of Service** configuration page displays. By default, the **General** tab displays. [Table 95](#) describes the fields and buttons on the **General** tab.

The screenshot shows the 'Class of Service: Scavenger' configuration page. The left sidebar lists various configuration categories, with 'Classes of Service' selected. The main area is titled 'Class of Service: Scavenger' and has a 'General' tab selected. The configuration fields are as follows:

- Core:** Name: Scavenger
- Marking:**
 - Use Legacy Priority Override defined in the WLAN Service
 - 802.1p Priority: Priority 0 (dropdown)
 - ToS/DSCP: 0x (DSCP:) (Select) Mask: 0x FF
- Rate Limiting:**
 - Inbound Rate Limit: (dropdown) Edit New
 - Outbound Rate Limit: (dropdown) Edit New
- Transmit Queue Assignment:**
 - Transmit Queue: Transmit Queue 0 (dropdown)

Buttons for 'New' and 'Save' are located at the bottom of the configuration area.

Table 95: General Tab - Fields and Buttons

Field/Button	Description
Core	
Name	Enter a name to assign to this class of service.
Marking	
Use Legacy Priority Override defined in the WLAN Service	Priority override allows you to define and force the traffic to a desired priority level. Priority override can be used with any combination. You can configure the service class and the DSCP values. Select this checkbox to use Priority Override defined in the WLAN as in previous releases. For more information, see Configuring the Priority Override on page 323.
802.1p Priority	Select this checkbox to define how the Layer 2 priority of the packet will be marked. From the drop-down list, select Priority 0 to Priority 7. For more information, see Priority and ToS/DSCP Marking on page 443. Note: This selection is not available if Legacy Priority Override is checked.

Table 95: General Tab - Fields and Buttons (continued)

Field/Button	Description
ToS/DSCP Marking	Select this checkbox to define how the Layer 3 ToS/DSCP will be marked. Enter a hexadecimal value in the 0x (DSCP:) field, or Click the Select button to open the ToS/DSCP Configuration dialog. For more information, see Configuring ToS/DSCP Marking on page 443. Note: Note: This selection is not available if Legacy Priority Override is checked.
Mask: 0x	Displays the hexadecimal value to use for the ToS/DSCP value. For example, if the mask is 0xF0, then only the four most significant bits of the ToS of the received packets are marked. So, if the received ToS is 0x33 and the ToS marking is set to 0x2A, then the resulting ToS is 0x23.
Rate Limiting	
Inbound Rate Limit	Select this checkbox, and then select an inbound rate limit from the drop-down list or click the New button to create a new inbound rate limit profile. To edit an existing inbound rate limit profile, select the profile from the drop-down list and then click the Edit button. For more information, see Rate Limiting on page 444.
Outbound Rate Limit	Select this checkbox, and then select an outbound rate limit from the drop-down list or click the New button to create a new outbound rate limit profile. To edit an existing outbound rate limit profile, select the profile from the drop-down list and then click the Edit button. For more information, see Rate Limiting on page 444.
Transmit Queue Assignment	
Transmit Queue	Select this checkbox, and select a Transmit Queue from the drop-down list. The Transmit Queue assignment is an override to the default TXQ assignment specified in the 802.1p priority, but without remarking the actual 802.1p field.

CoS Rule Classification

Classification is the process of finding the first matching rule that defines a for an incoming packet. The order of classification is as follows:

- 1 Use the CoS assigned by the first role rule matched by the packet that explicitly assigns a CoS.
- 2 If no CoS found, use the default CoS of the Role.
- 3 If still no CoS found, use the default CoS of the WLAN (for non-auth role).

For inbound traffic, classification is done at the AP (if AP Filtering is enabled), otherwise it is done at the controller. For outbound traffic, classification is always done at the controller.

The Rule that assigns authorization (Access Control) may not be the same rule that assigns CoS. Therefore, up to two passes are made through the policy rules for each packet. If the first pass results in the packet being allowed a second pass will take place to classify the packet for CoS.

- The first pass looks for authorization (allow, deny).
- The second pass classifies and assigns the CoS.

The number of rules reported to Policy Manager are limited to the number of rules allowed on the controller. On the controller, a single rule can contain different classification types whereas for Policy Manager this rule may be split into several rules. For example, if a rule defines an IP source address and also a ToS value, then this rule would be split into an IP type and a ToS type. Rules exceeding the limit after splitting will be dropped.

Priority and ToS/DSCP Marking

After packets are classified, they are assigned a final User Priority (UP) value. The Priority and ToS/DSCP Marking bits to be applied to the packet is taken from the and if not set, the received value (ToS/DSCP) is used. ToS/DSCP Marking rewrites the Layer 3 Type of Service (ToS) byte.

Configuring ToS/DSCP Marking

To configure ToS/DSCP marking:

- 1 From the **Class of Service General** tab, click **ToS/DSCP Marking**.
- 2 Click the **Select** button.

The **ToS/DSCP Configuration** dialog displays:



Note

Select either **Type of Service (ToS)** or **Diffserv Codepoint (DSCP)** from this dialog. You cannot configure both types.

- 3 If you select **Type of Service (ToS)**:
 - a Select a Precedence value from the drop-down list.
 - b Select a specific ToS from the following list:
 - Delay Sensitive
 - High Throughput
 - High Reliability
 - Explicit Congestion Notification
- 4 If you select **Diffserv Codepoint (DSCP)**:
 - Choose a Well-known Value, or
 - Enter a Raw Binary Value
- 5 Close the **Configuration** dialog.

The logic used to find the final User Priority (UP) depends on the , the received UP, or the final ToS/DSCP value. Here are the steps followed to determine the final UP:

- 6 Use UP markings defined in CoS (directly or via Legacy UP override).
- 7 If still no UP, use UP from the received packet.
- 8 If still no UP, use DSCP marking defined in CoS and map to UP with WLANs DSCP-to-UP mapping table.
- 9 If still no UP, use received DSCP value and map to UP with WLANs DSCP-to-UP mapping table.

Rate Limiting

The Inbound and Outbound Rate Limit is enforced on a per-station basis whether the rate limit is assigned to a rule, role or WLAN. Each station has its own set of counters that are used to monitor its wireless network utilization. Traffic from other stations never count against a station's rate limits.

- Controllers support up to 128 system wide rate profiles when managed from the controller.
- Each role can use a maximum of 9 inbound rate profiles and 9 outbound rate profiles. For each direction there can be one rate profile assigned by the role's default and 8 other rate profiles assigned by the role's rules.
- There is no limit to how many rules allow CoS assignments as long as there are never more than 8 + 8 rate profiles assigned by Classes of Service.

If two or more rules in the same role assign the same named rate profile to a station's packets, then those rules "share" the rate profile. In [Figure 107](#), a role's rules assign both HTTP and FTP traffic to the same rate limiter. The sum of the amounts of HTTP and FTP traffic determine whether the rate limit is being exceeded. Each station gets its own set of rate limiters. So the HTTP and FTP traffic of other stations never gets counted against a station's own rate profile limits.

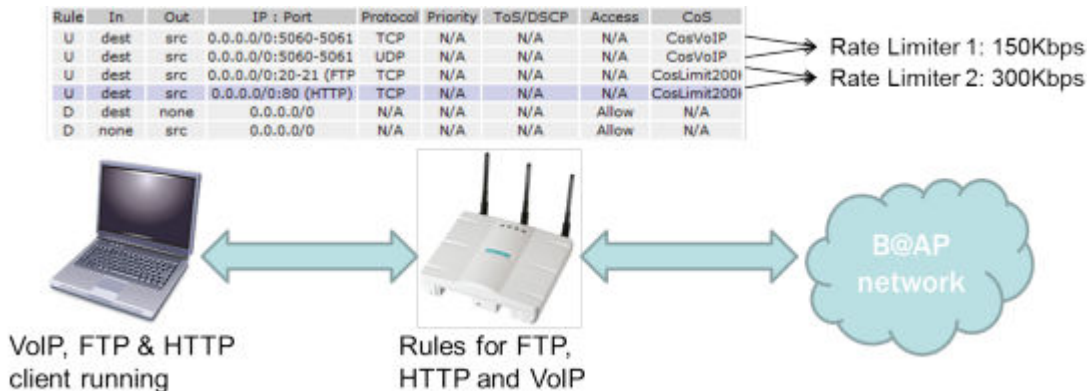


Figure 107: Rate Limiter Example

10 Configuring Sites

VNS Sites Overview
Configuring Sites
Recommended Deployment Guidelines
Radius Configuration
Selecting AP Assignments
Selecting WLAN Assignments

VNS Sites Overview

A Site is a mechanism for grouping APs and refers to specific Roles, and RADIUS servers that are grouped to form a single configuration. Sites allow for deployment where the authentication server is local and provides the ability to associate a new 802.1x client and to allow 802.1x clients to roam with Fast Roaming when the AP's home controller is unreachable.

When configuring a Site profile, two additional tabs are included:

- An AP Assignments tab provides a list of APs that can be assigned to a specific Site. Once an AP is assigned, the controller preloads the APs with the server configuration used by the Site.
- A WLAN Assignments tab lists available WLANs and specific Radio assignments. WLAN Services can be assigned in the same way as AP Load Groups (see [Configuring Co-Located APs in Load Balance Groups](#) on page 187).

Configuring Sites

Topology groups for sites is not supported. You can add a WLAN or Role to a site if it does not use a topology group. You can change the configuration of a WLAN, Role, and VNS to use a topology group, but if the WLAN, Role, or VNS is part of the Site configuration, the Site configuration will become invalid. At that point, you must remove the topology group related configuration from the site configuration.

A site can also use any Bridged at AP, Bridged at Controller, or Routed Topology defined in the controller. Once an AP is assigned to a site, the controller will preload the AP with Topologies, Roles, and RADIUS server configuration used by the site. The AP will then be able to use these configuration items even when the controller is unreachable.

An AP that is part of a site that has local RADIUS client services enabled will use its own RADIUS client to do the following:

- Perform all MAC-based authentication for all stations associated with it on any of the WLAN Services assigned to it.
- Perform all RADIUS server interactions for 802.1x authentications for all stations associated with it on any 802.1x WLAN Service assigned to it.

Recommended Deployment Guidelines

The Sites feature introduces new and complex interactions between hardware and software components. Sites are recommended for customers who have an AP-to-controller link (in a normal deployment) which they expect will be disconnected for long periods of time, but still expect to give service to users.

**Note**

For best performance and maintainability, do not use the Sites feature if the AP-to-controller link is normally connected.

The following guidelines are recommended to configure a secure and easy-to-maintain Site:

- Use 802.1x and WPA2 Enterprise authentication and privacy.
- Do not use MAC-based authentication (MBA) unless absolutely required.
- Do not use more than 32 policy rules within a single AP filter.
- Do not configure a Sites AP Session Availability function without an AP-to-controller link.
- Do not configure the following features in a Sites configuration since they rely on a consistent AP-to-controller link:
 - Tunneled/Routed topologies
 - RADIUS accounting
 - Captive Portal

Defining Roles, CoS, and RADIUS Servers for Local RADIUS Authentication

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

- In the left pane, click **Sites**. The **sites** screen displays.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A Logout link is in the top right. The left sidebar has a 'New...' button and a 'Global' section with 'Sites' selected. Below 'Global' are 'Site-EWC', 'Site-Local', and 'SiteLocal'. Further down are 'Virtual Networks', 'WLAN Services', 'Roles', 'Classes of Service', and 'Topologies'. The main content area is titled 'Sites' and contains a table with the following data:

Name	Local RADIUS	Band Pref.	Secure Tunnel	APs Assigned	WLANs Assigned
<input type="checkbox"/> Site-EWC	x	x	x	0	1
<input type="checkbox"/> Site-Local	x	x	x	0	2
<input type="checkbox"/> SiteLocal	x	x	✓	0	0

Below the table are two buttons: 'New' and 'Delete Selected'.

- In the left pane, click the name of the Site that you want to edit, or click the **New** button to create a new Site. The **Site** configuration page displays. By default, the **Configuration** tab displays. [Table 96](#) describes the fields and buttons on the Configuration tab.

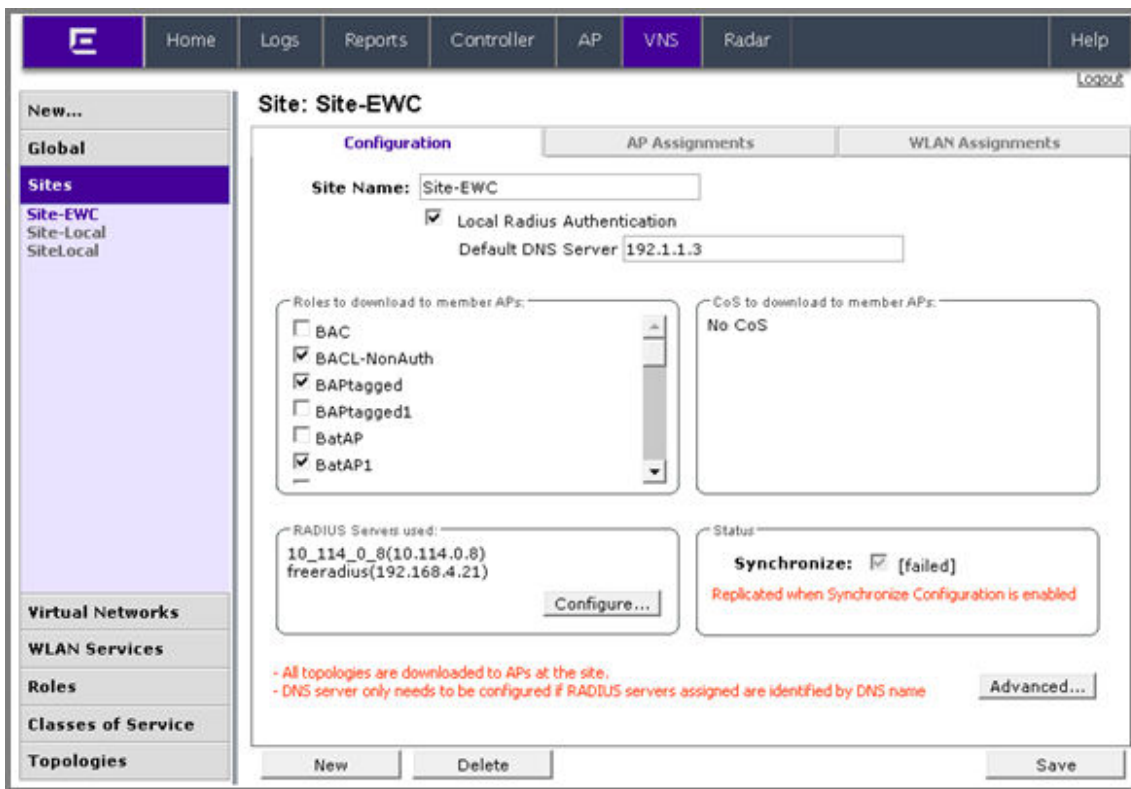


Table 96: Configuration Tab - Fields and Buttons

Field/Button	Description
Site Name	Enter a name to assign to this Site. The name is unique among Sites on the controller. AP load group names and Site names are part of the same space so a load group and a Site cannot have the same name.
Local Radius Authentication	Select this checkbox to choose a local RADIUS Server for login credentials and authentication.
Default DNS Server	This field is used to resolve RADIUS server names to IP addresses if necessary.
Roles to download to member APs	Select roles that will be applied to APs with this specific Site configuration. Physical topologies and third party AP enabled topologies cannot be assigned to a Site.
to download to member APs	Displays the Class of Service that will be applied to APs with this specific Site configuration.
RADIUS Server used	Displays the list of available RADIUS servers used for this Site (for more information, see Radius Configuration on page 451). The RADIUS servers assigned to a Site override the list of RADIUS servers in the WLAN Service definition for APs that are part of the Site.

Table 96: Configuration Tab - Fields and Buttons (continued)

Field/Button	Description
Status: Synchronize: (unknown)	Select this checkbox to enable automatic synchronization with an availability peer. Refer to Using the Sync Summary on page 365 for information about viewing synchronization status. If this Site is part of an availability pair, Extreme Networks recommends that you enable this feature.
Advanced Button	
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> <p>Disabled — Secure Tunnel is turned off and no traffic is encrypted. All SFTP/SSH/TFTP traffic works normally.</p> <p>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.</p> <p>Encrypt control and data traffic between AP & Controller — This mode only benefits routed/bridged@AP 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> <p>Note: This option is not available for AP3805 models.</p> <p>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> <p>Note: Changing a Secure Tunnel mode will automatically disconnect and reconnect the AP.</p>
Secure Tunnel Lifetime	<p>When Secure Tunnel is enabled, enter an interval (in hours) at which time the keys of the IPSEC tunnel are renegotiated. Only applies if both the AP and controller are running V8.31 or newer.</p> <p>Note: Changing the Secure Tunnel Lifetime setting will not cause any AP disruption.</p>
Encrypt control traffic between APs	Select checkbox to provide encryption, authentication, and key management between APs and/or controllers.
Band Preference	Select this checkbox to enable APs to become members of both this Site and a load group at the same time.

Table 96: Configuration Tab - Fields and Buttons (continued)

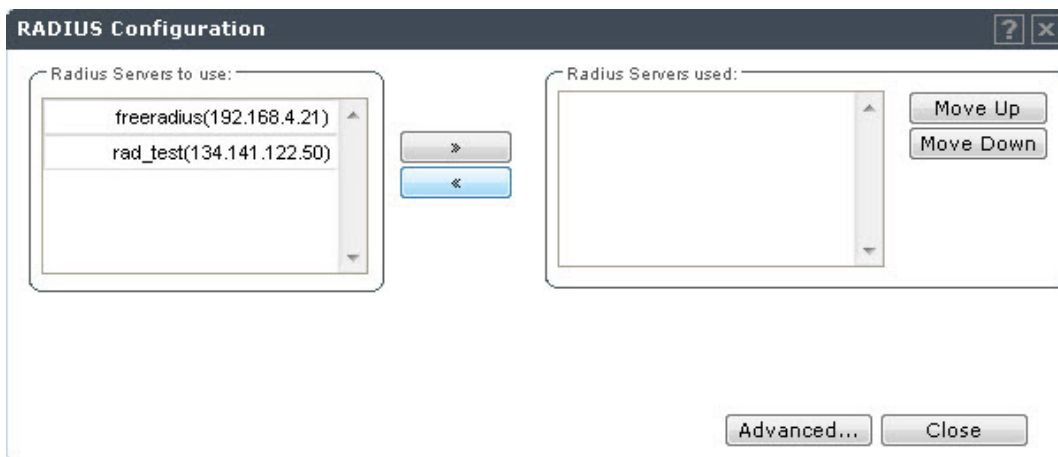
Field/Button	Description
Load Control	<p>Select the following parameters for each radio assigned to this Site:</p> <ul style="list-style-type: none"> • Enable: Select this checkbox to enable Radio Load Control (RLC) for individual radios (Radio1 and Radio2) associated with this Site. • Max. # of Clients: 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 checkbox 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.
RADIUS Authentication: Replace Called Station ID with Zone	Select this checkbox to allow the RADIUS client to send the AP Zone as the Called-Station ID instead of the radio MAC address. This feature can be enabled regardless of whether the Site is using centrally located or local RADIUS servers.

Radius Configuration

A single Site definition can be configured with one or two RADIUS servers. The RADIUS servers assigned to a Site can only be selected from the list of servers displayed on the **RADIUS Configuration** dialog.

To select site RADIUS servers:

- 1 From the **Configuration** tab, under RADIUS Server used, click **Configure**. The **RADIUS Configuration** dialog displays.



- 2 Select a RADIUS server from the list of available servers and click the right-arrow button.

The server will be moved under the RADIUS Servers used list.
- 3 Click the **Move Up** or **Move Down** buttons to change the order of the RADIUS Servers used.
- 4 Click the **Advanced** button. The **RADIUS Advanced Configuration** dialog appears.

RADIUS Advanced Configuration ? X

NAS IP Address: Use VNS IP address or use:

NAS identifier: Use VNS name or use:

Auth. type:

Password:

Note: RADIUS Password override is for MBA only

- 5 The following values can be edited:
 - NAS IP Address — Click the checkbox to use the existing IP address of the VNS server, or enter an alternate IP Address in the box provided.
 - NAS Identifier — Click the checkbox to use the name of the existing VNS server, or enter an alternate name in the box provided.
 - Auth. type — Select an authorization protocol from the drop-down list (PAP, CHAP, MS-CHAP, or MS-CHAP2).
 - Password — To override the default password (see [VNS Global Settings](#) on page 345) for MBA - MAC Based authorization only. Select Mask to display the password, and select Unmask to hide the entry.
- 6 Click **Close**.

Selecting AP Assignments

To Select AP Assignments:

- 1 Click the **AP Assignments** tab.

- 2 Select the APs to apply to the Site configuration.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A left sidebar contains a menu with options: New..., Global, Sites (selected), Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main content area is titled 'Site:' and has three tabs: Configuration, AP Assignments (selected), and WLAN Assignments. The 'AP Assignments' tab displays a table with the following data:

AP Name	
3715e	<input type="checkbox"/>
3825i	<input type="checkbox"/>
3865e	<input type="checkbox"/>
3935i	<input type="checkbox"/>
name-1331061908500000	<input type="checkbox"/>
w781	<input type="checkbox"/>
w7811	<input type="checkbox"/>

A 'Save' button is located at the bottom right of the configuration area.

Selecting WLAN Assignments

To Select WLAN Assignments:

- 1 Click the **WLAN Assignments** tab.
- 2 Select Radio assignments (Radio 1 and Radio 2) for specific WLANs that will be applied to this Site configuration.

3 Click **Save**.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, **VNS**, Radar, and Help. A **Logout** link is visible in the top right. The left sidebar contains a navigation menu with the following items: New..., Global, **Sites**, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main content area is titled **Site:** and has three tabs: Configuration, AP Assignments, and **WLAN Assignments**. The **WLAN Assignments** tab displays a table with the following data:

WLAN Name	Radio 1	Radio 2
CNL-422-0-0	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-0-1	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-0-2	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-0-3	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-1-2-wds	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-1-4-wds	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-1-5	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-1-6	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-1-7	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-2-10	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-2-11	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-2-12-wds	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-2-8	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-2-9	<input type="checkbox"/>	<input type="checkbox"/>

A **Save** button is located at the bottom right of the configuration area.

11 Working with a Mesh Network

About Mesh

Simple Mesh Configuration

Wireless Repeater Configuration

Wireless Bridge Configuration

Examples of Deployment

Mesh WLAN Services

Key Features of Mesh

Deploying the Mesh System

Changing the Pre-shared Key in a Mesh WLAN Service

About Mesh

Mesh networks enable you to expand the wireless network by interconnecting the wireless APs through wireless links in addition to the traditional method of interconnecting wireless APs via a wired network. In a Mesh deployment, each node not only captures and disseminates its own data, but it also serves as a relay for other nodes, that is, it collaborates to propagate the data in the network.

A Mesh deployment is ideally suited for locations where installing Ethernet cabling is too expensive, or physically impossible.

The Mesh network can be deployed in three configurations:

- Simple Mesh Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration

Simple Mesh Configuration

In a typical Mesh configuration, the APs are connected to the distribution system via an Ethernet network, which provides connectivity to the ExtremeWireless Appliance.

However, when an AP is installed in a remote location and can't be wired to the distribution system, an intermediate AP is connected to the distribution system via the Ethernet link. This intermediate AP forwards and receives the user traffic from the remote AP over a radio link.

The intermediate AP that is connected to the distribution system via the Ethernet network is called Mesh portal, and the AP that is remotely located is called the Mesh AP.

The following figure illustrates the Simple Mesh configuration:

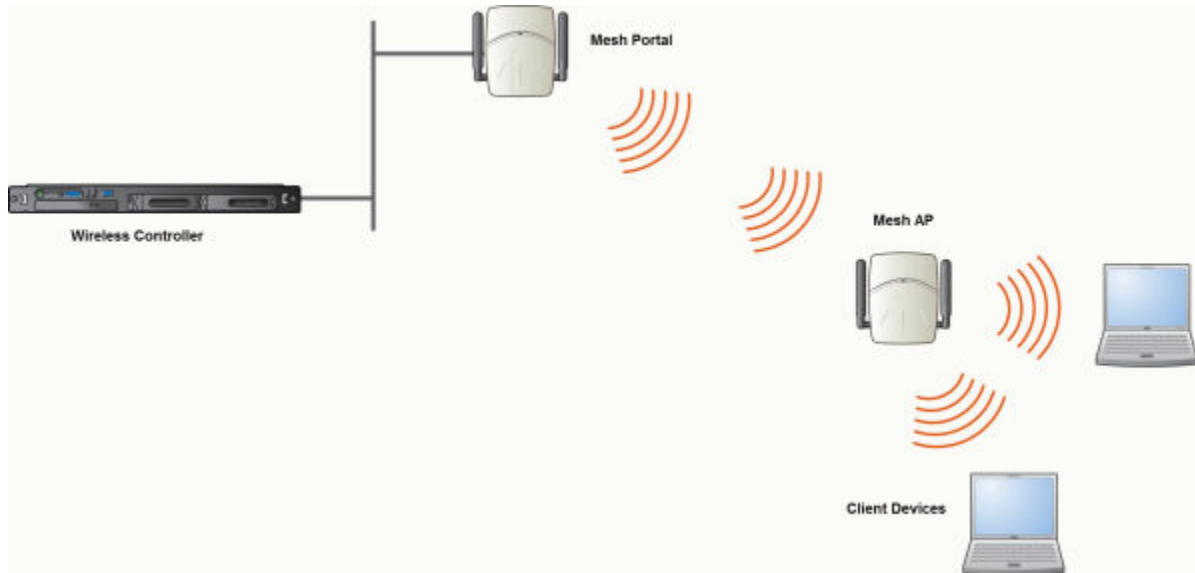


Figure 108: Simple Mesh Configuration

Wireless Repeater Configuration

In Wireless Repeater configuration, a Mesh AP is installed between the Mesh Portal and the destination Mesh AP. The Mesh AP relays the user traffic between the Mesh Portal and the destination Mesh AP. This increases the WLAN range.

Figure 109 illustrates the Wireless Repeater configuration:

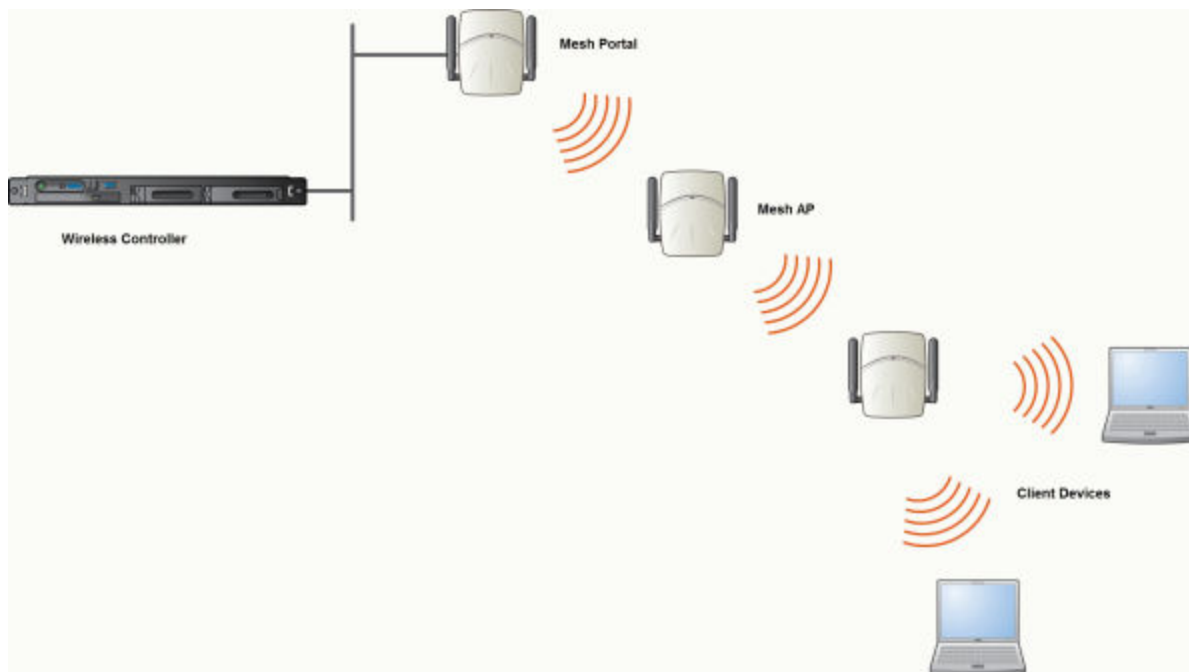


Figure 109: Wireless Repeater Configuration



Note

You should restrict the number of repeater hops in a Wireless Repeater configuration to three for optimum performance.

Wireless Bridge Configuration

In Wireless Bridge configuration, the traffic between two APs that are connected to two separate wired LAN segments is bridged via Mesh link. You may also install a Mesh AP between the two Wireless APs connected to two separate LAN segments.

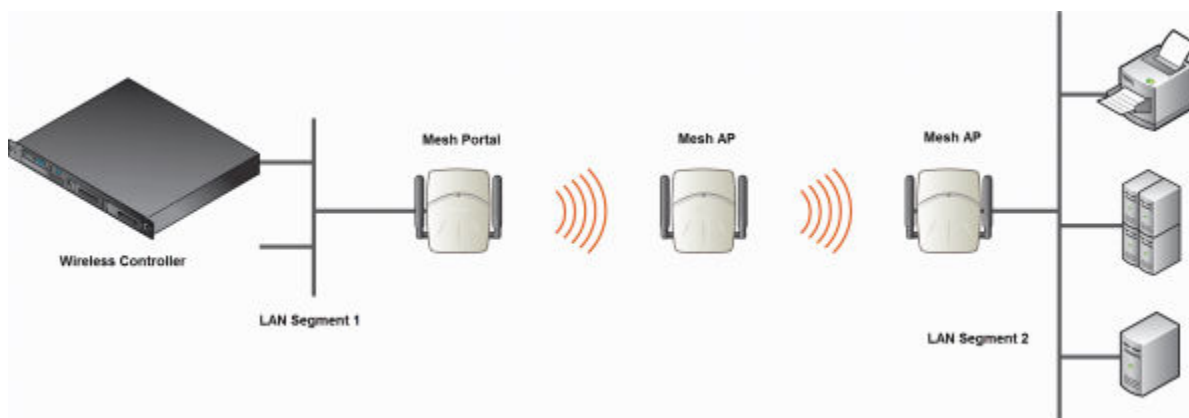


Figure 110: Wireless Bridge Configuration

When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Mesh AP is connected to the wired LAN.

Examples of Deployment

The following illustration depicts a few examples of Mesh deployment.

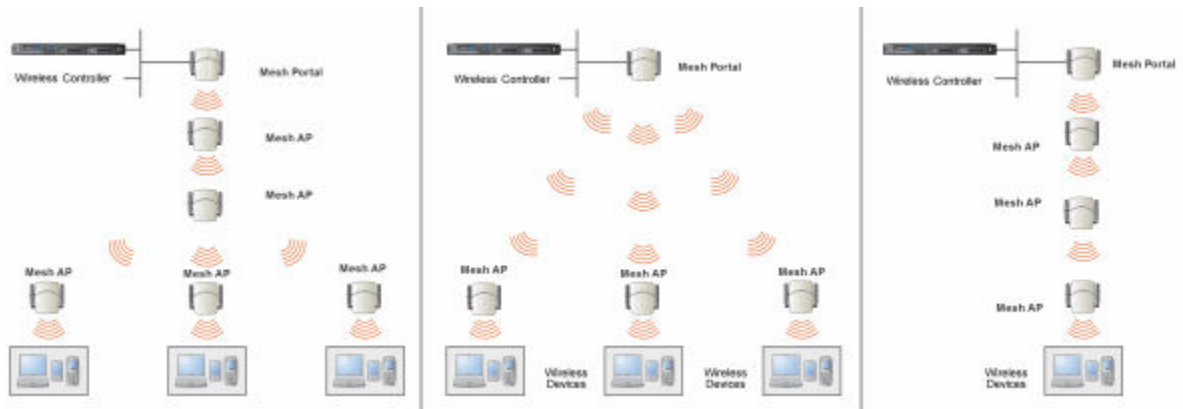


Figure 111: Examples of Mesh Deployment

Mesh WLAN Services

In a traditional WLAN deployment, each radio of the AP can interact with the client devices on a maximum of eight networks.

In Mesh deployment, one of the radios of every Mesh AP establishes a Mesh link on an exclusive WLAN Service. The Mesh AP is therefore limited to seven network WLAN Services on the Mesh radio. The other radio can interact with the client-devices on a maximum of eight WLAN Services.

The WLAN Service on which the APs establish the Mesh link is called the Mesh WLAN Service.

A Mesh can be setup either by using either a single Mesh WLAN Service or multiple Mesh WLAN Services. The following figures illustrate the point.

In [Figure 112](#) on page 459:

- The rectangular enclosure denotes an office building.
- The four wireless APs — Minoru, Yosemite, Bjorn and Lancaster — are within the confines of the building and are connected to the wired network.
- The space around the office building is a warehouse.
- The solid arrows point towards Current Parents.
- The dotted arrows point towards Alternative Parents.

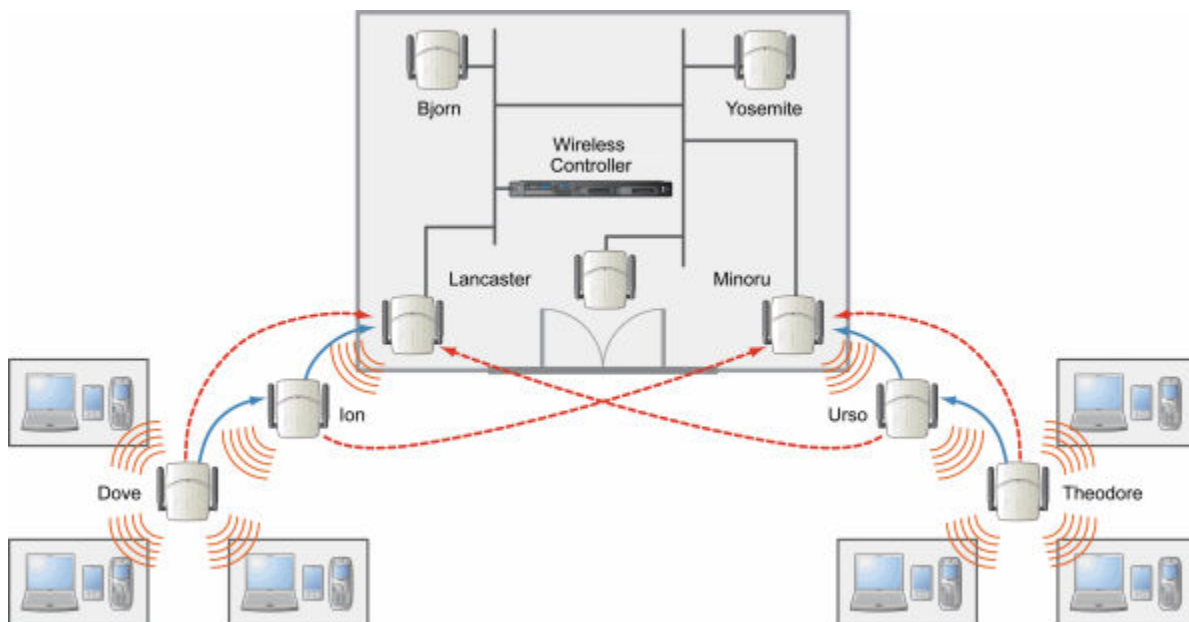


Figure 112: Deployment Example

Mesh Setup with a Single Mesh WLAN Service

Deploying the Mesh for the above example using a single Mesh WLAN Service results in the following structure shown in [Figure 113](#).

The tree will operate as a single Mesh entity. It will have a single Mesh SSID and a single pre-shared key for Mesh links. This tree will have multiple roots. For more information, see [Multi-Root Mesh Topology](#) on page 464.

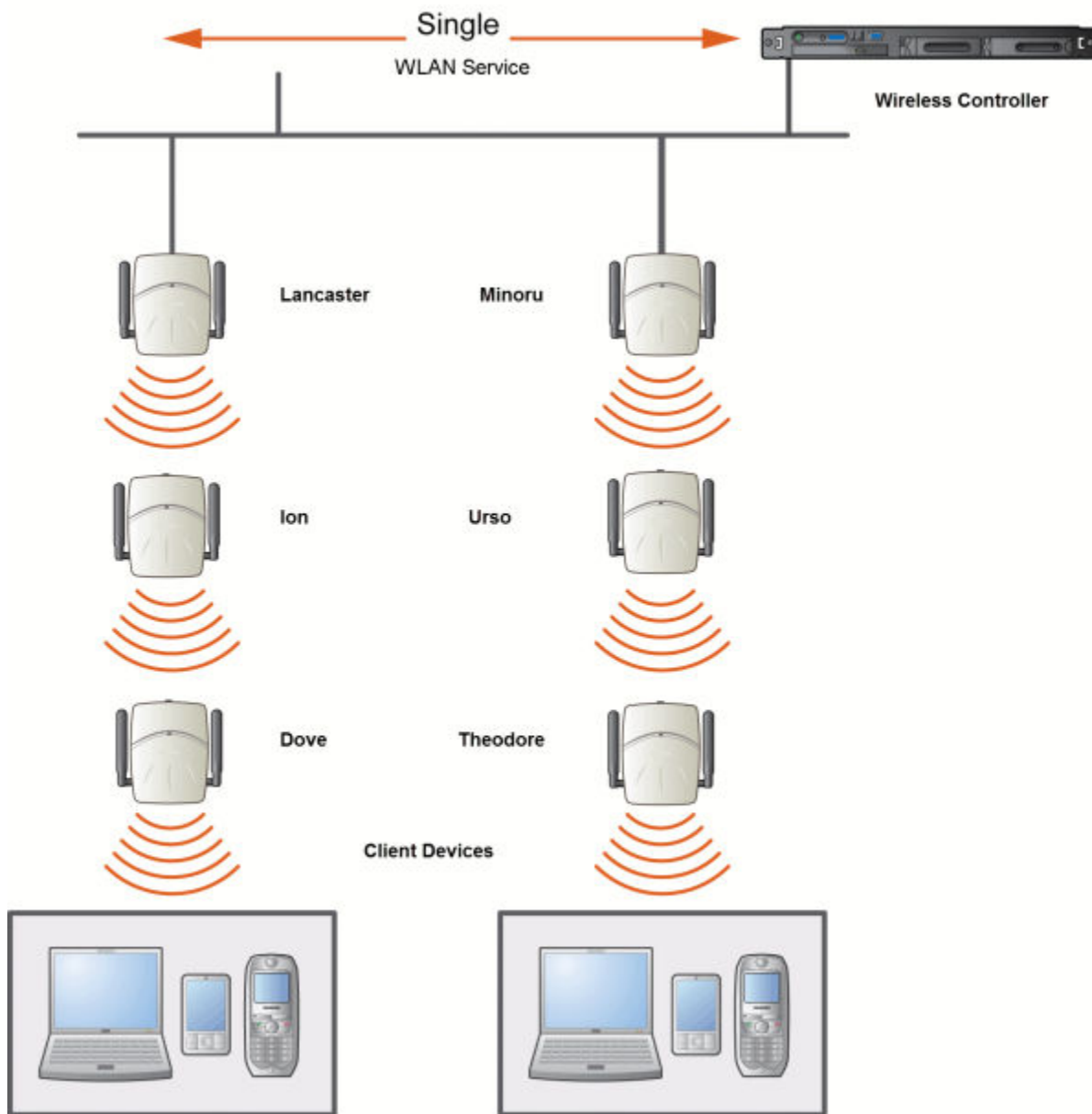


Figure 113: Mesh Setup with a Single Mesh WLAN Service

Mesh Setup with Multiple Mesh WLAN Services

You can also deploy the same Mesh in [Figure 112](#) on page 459 using two Mesh WLAN Services. The Two Mesh WLAN Services will create two independent Mesh trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

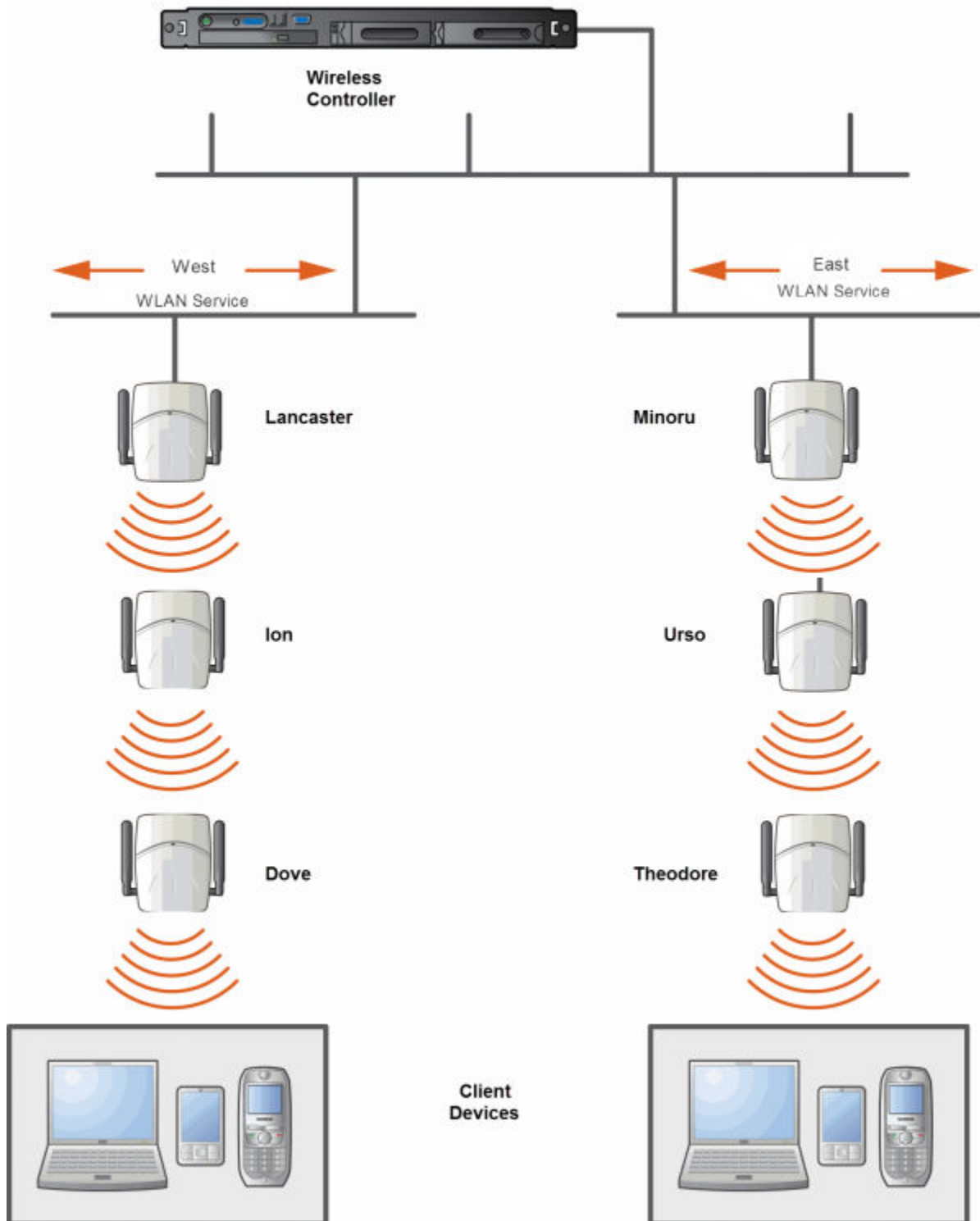


Figure 114: Mesh Setup with Multiple Mesh WLAN Services

Key Features of Mesh

Some key features of Mesh are:

- [Self-Healing Network](#) on page 462
- [Tree-like Topology](#) on page 462
- [Radio Channels](#) on page 463
- [Multi-Root Mesh Topology](#) on page 464
- [Figure 116](#) on page 464

Self-Healing Network

Data in a Mesh network propagates along a path, by hopping from node to node until the destination is reached. To ensure that all its paths' availability, the Mesh network allows for continuous connections and reconfiguration around broken or blocked paths, referred to as self-healing. The self-healing capability enables a routing based network to operate when one node breaks down or a connection goes bad.

Tree-like Topology

The APs in Mesh configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Mesh Portal being the tree root, and the Mesh AP being the tree leaves.

The nodes in the tree-structure have a parent-child relationship. The Mesh AP dynamically selects the best parent for connecting to the Mesh portal. A Mesh AP can have the role of both parent and child at the same time and the AP's role can change dynamically.

[Figure 115](#) on page 463 illustrates the parent-child relationship between the nodes in a Mesh topology.

- Mesh Portal is the parent of Mesh AP 1.
- Mesh AP 1 is the child of Mesh Portal.
- Mesh AP 1 is the parent of Mesh AP 2.
- Mesh AP 2 is the child of Mesh AP 1.
- Mesh AP 2 is the parent of the following Wireless APs:
 - Mesh AP 5
 - Mesh AP 4
 - Mesh AP 3
- All the three Mesh APs are the children of Mesh AP 2.

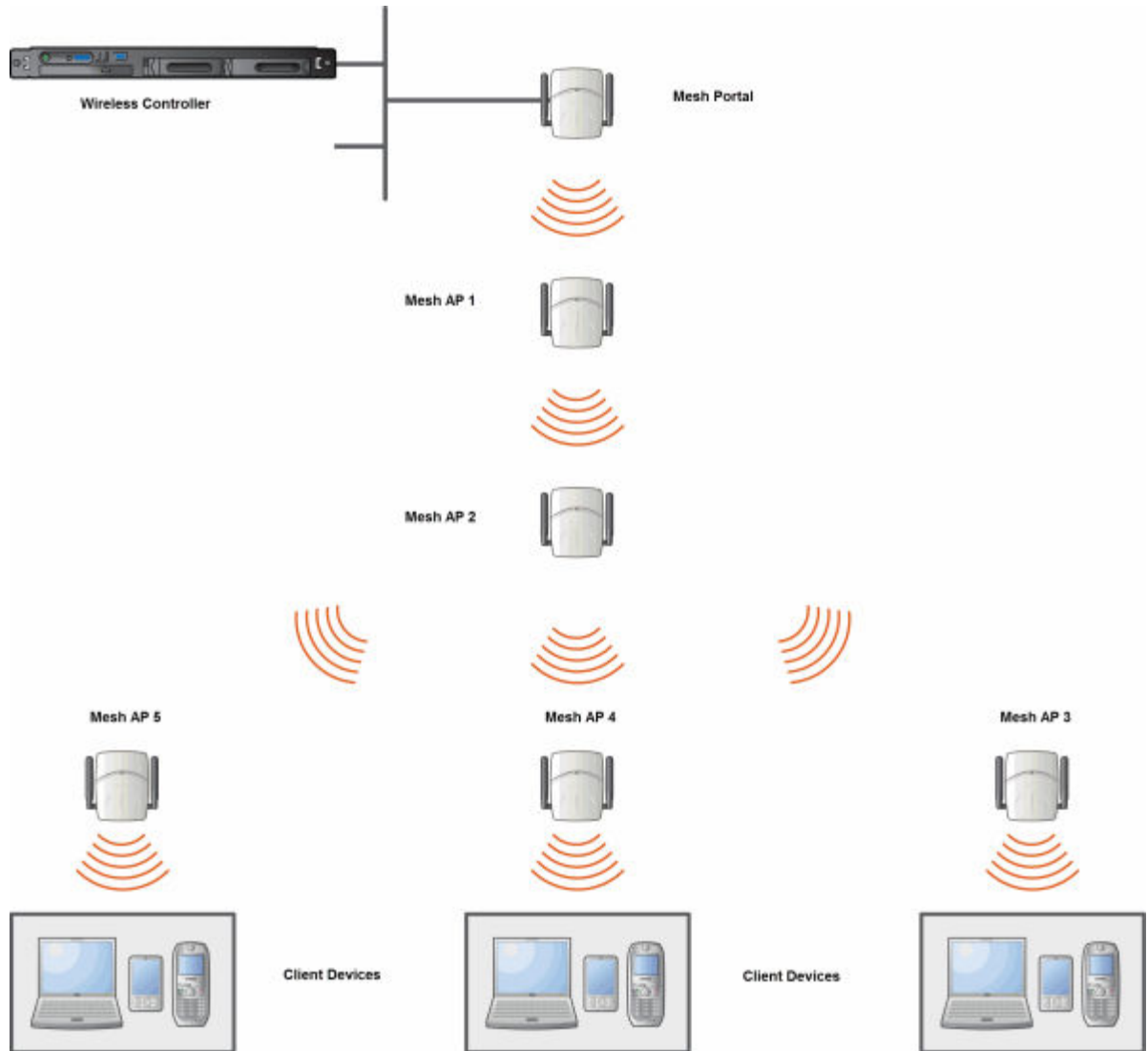


Figure 115: Parent-Child Relationship Between Wireless APs in Mesh Configuration



Note

If an AP is configured to serve as a scanner in Radar, it cannot be used in a Mesh tree. For more information, see [Working with ExtremeWireless Radar](#) on page 517.



Note

It is recommended that you limit the number of APs participating in a Mesh tree to 50. This limit guarantees decent performance in most typical situations.

Radio Channels

All APs in a mesh deployment must have Mesh configured on the same radio. On the backhaul radio, the following settings must be set the same way for all APs in the Mesh:

- Radio mode

- Minimum Basic Rate

Multi-Root Mesh Topology

A Mesh topology can have multiple Mesh Portals. Figure 116 illustrates the multiple-root Mesh topology.

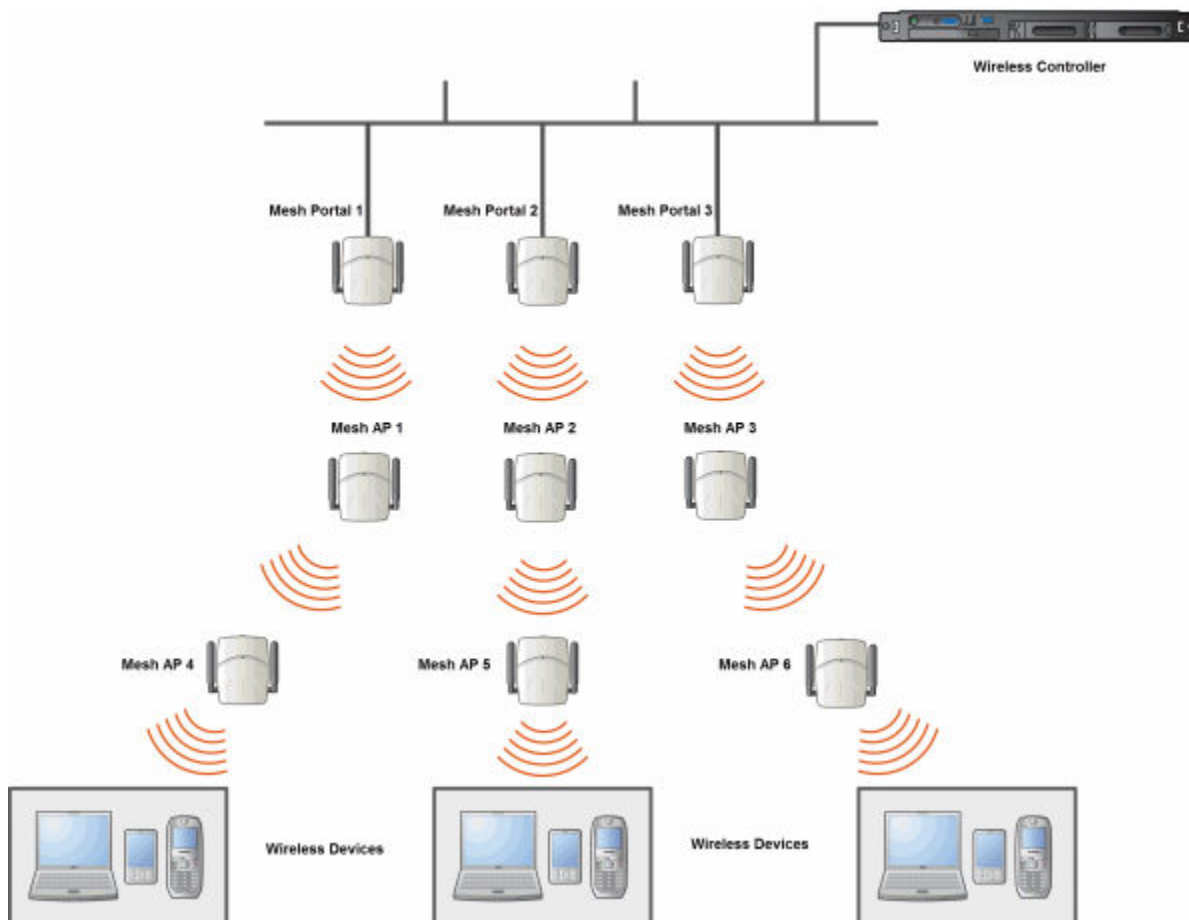


Figure 116: Multiple-Root Mesh Topology

Link Security

The Mesh link is encrypted using Advance Encryption Standard (AES).



Note

The keys for AES are configured prior to deploying the Repeater or Mesh APs.

Deploying the Mesh System

Before you start configuring the Mesh APs, you must ensure the following:

- The APs that are part of the wired WLAN are connected to the wired network.

- The wired APs that will serve as the Mesh Portal of the proposed Mesh topology are operating normally.
- The WLAN is operating normally.

Planning the Mesh Topology

You may sketch the proposed WLAN topology on paper before you start the Mesh deployment process. You should clearly identify the following in the sketch:

- Mesh APs with their names
- Radios that you will choose to link the APs

Provisioning the Mesh Wireless AP

This step is of crucial importance and involves connecting the Mesh APs to the enterprise network via the Ethernet link. This is done to enable the Mesh APs to connect to the wireless controller so that they can derive their Mesh configuration.

The Mesh AP's configuration includes pre-shared key and its role, preferred parent name and the backup parent name.



Note

The provisioning of Mesh APs must be done before they are deployed at the target location. If the APs are not provisioned, they will not work at their target location.

Mesh Deployment Overview

The following is the high-level overview of the Mesh deployment process:

- 1 Connecting the Mesh APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the wireless controller. For more information, see [Discovery and Registration](#) on page 119.
- 2 Disconnecting the Mesh APs from the enterprise network after they have discovered and registered with the wireless controller.
- 3 Creating a Mesh VNS.
- 4 Assigning roles, parents and backup parents to the Mesh wireless APs.
- 5 Assigning the Mesh APs' radios to the network VNSs.
- 6 Connecting the Mesh APs to the enterprise network via the Ethernet link for provisioning. For more information, see [Provisioning the Mesh Wireless AP](#) on page 465.
- 7 Disconnecting the Mesh APs from the enterprise network and moving them to the target location.



Note

During the Mesh deployment process, the Mesh APs are connected to the enterprise network on two occasions — first to enable them to discover and register with the wireless controller, and then the second time to enable them to obtain the provisioning from the wireless controller.

Connecting the Mesh APs to the Network for Discovery and Registration

Connect each Mesh wireless AP to the enterprise network to enable it to discover and register itself with the wireless controller.

Note



Before you connect the Mesh APs to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the wireless controller is defined according to your security needs. The **Security mode** property dictates how the wireless controller behaves when registering new and unknown devices. For more information, see [Wireless AP Registration](#) on page 121. If the **Security mode** is set to **Allow only approved Wireless APs to connect** (this is also known as secure mode), you must manually approve the Mesh APs after they are connected to the network for the discovery and registration. For more information, see [New Button -- Adding and Registering a Wireless AP](#) on page 128.

Depending upon the number of Ethernet ports available, you may connect one or more Mesh wireless APs at a time, or you may connect all of them together.

Once a Mesh wireless AP has discovered and registered itself with the wireless controller, disconnect it from the enterprise network.

Configuring the Mesh Wireless APs Through the Controller

Configuring the Mesh wireless APs involves the following steps:

- 1 Creating a Mesh WLAN Service.
- 2 Defining the SSID name and the pre-shared key.

For ease of understanding, the Mesh configuration process is explained with an example. [Figure 117](#) on page 467 depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four APs — Ardal, Arthur, Athens and Auberon — are within the confines of the building, and are connected to the wired network.
- The space around the building is the warehouse.
- The solid arrows point toward Current Parents.
- The dotted arrows point toward Alternative Parents.

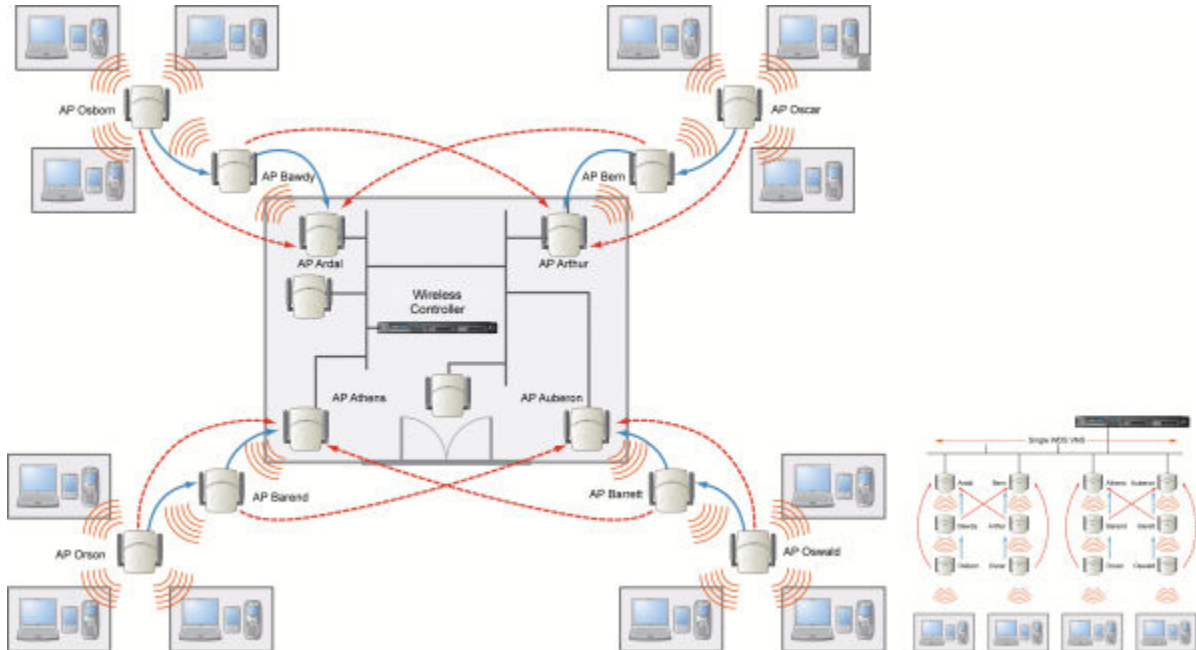


Figure 117: Mesh Deployment

Note



With the single Mesh VNS, the tree structure for the Mesh deployment will be as depicted on the bottom right of [Figure 117](#). You can also implement the same deployment using four Mesh VNSs, each for a set of APs in the four corners of the building. Each set of APs will form an isolated topology and will operate using a separate SSID and a separate Pre-shared key. For more information, see [Figure 111](#) on page 458.

To Configure the Mesh wireless APs through the controller:

Before configuring Mesh, be sure that the following conditions are met:

- Energy Save is set to Off
- Beacon Interval is set to 100 msec
- AP names are 32 characters or less for statistics display purposes
- ATPC and DCS are both disabled.

If possible, follow these guidelines for the backhaul radio to achieve a balance of stability, throughput, and latency:

- Use a 5.2 GHz band for backhaul
- Select a non-DFS channel for the Mesh Portal
- Use a 40 MHz Channel Width and Short guard interval
- Disable Aggregate MSDUs
- Enable Aggregate MPDUs
- Enable ADDBA support
- Configure the settings on the Radio configuration page the same for all APs in the Mesh.
- Set the Poll Timeout to be at least 60 seconds.

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the **WLAN Services** pane and select a Mesh service to edit or click the **New** button.
- 3 Enter a name for the service in the **Name** field.
- 4 The **SSID** field is automatically filled in with the name, but you can change it if desired.
- 5 For **Service Type**, select **Mesh**.

The screenshot shows the 'WLAN Services' configuration page. The left sidebar lists various service IDs under 'WLAN Services'. The main configuration area is titled 'WLAN:' and contains a 'WLAN Services' section. Under 'Config', there is a 'Name' text field, a 'Service Type' section with radio buttons for Standard, WDS, Mesh (selected), Third Party AP, and Remote, and an 'SSID' text field. Under 'Status', there is an 'Enable' checkbox which is checked. A 'Save' button is located at the bottom right of the configuration area.

- 6 To save your changes, click **Save**. The **WLAN configuration** window is re-displayed to show additional configuration fields.

WLAN: Test

WLAN Services

Core

Name:

Service Type: Mesh

SSID:

Mesh Settings

Pre-shared Key:

Backhaul Radio:

Status

Enable:

Wireless APs services

AP Name	Mesh Service	Bridge to LAN	Radio #
C4110 - ap2 - AP3620	<input type="text" value="none"/>	<input type="checkbox"/>	1
C4110 - ap3 - AP3825e	<input type="text" value="none"/>	<input type="checkbox"/>	1

Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.

- 7 In the **Mesh Pre-shared Key** box, type the key.



Note

The pre-shared key must be 8 to 63 characters long. The Mesh APs use this pre-shared key to establish a Mesh link between them.



Note

Changing the pre-shared key after the Mesh is deployed can be a lengthy process. For more information, see [Changing the Pre-shared Key in a Mesh WLAN Service](#) on page 470.

- 8 Assign a backhaul radio.



Note

After you save the configuration, you cannot change the backhaul radio. Please configure this setting wisely.

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



Note

The **Mesh Bridge** feature on the user interface relates to Mesh Bridge configuration. When you are configuring the **Mesh Bridge** topology, you must select Mesh Bridge for Mesh AP that is connected to the wired network. For more information, see [Wireless Bridge Configuration](#) on page 457.

Connecting the Mesh Wireless APs to the Enterprise Network for Provisioning

You must connect the Mesh wireless APs to the enterprise network once more to enable them to obtain their configuration from the wireless controller. The configuration includes the pre-shared key, the AP's role, preferred parent and backup parent. For more information, see [Provisioning the Mesh Wireless AP](#) on page 465.



Warning

If you skip this step, the Mesh APs will not work at their target location.

Moving the Mesh Wireless APs to the Target Location



Note

If you change any of the following radio properties of a Mesh AP, the Mesh AP will reject the change: disabling the radio on which the Mesh link is established, lowering the radio's Tx Power of a radio on which the Mesh link is established, or changing the country.

- 1 Disconnect the Mesh APs from the enterprise network, and move them to the target location.
- 2 Install the Mesh APs at the target location.
- 3 Connect the APs to a power source. The discovery and registration processes are initiated.

Changing the Pre-shared Key in a Mesh WLAN Service

To Change the Pre-shared Key in a Mesh WLAN Service

- 1 Create a new Mesh WLAN Service with a new pre-shared key.
- 2 Assign the RF of the APs from the old Mesh to the new Mesh WLAN Service.
- 3 Wait at least 30 seconds to ensure that all APs got the configuration, then disable the old Mesh WLAN service.
- 4 Check the **Mesh Statistics** report page to ensure that all the Mesh APs have connected to the wireless controller via the new Mesh VNS. For more information, see [Viewing Statistics for APs](#) on page 572.
- 5 Delete the old Mesh WLAN Service. For more information, see [Deleting a VNS](#) on page 438.

12 Working with a Wireless Distribution System

About WDS
Simple WDS Configuration
Wireless Repeater Configuration
Wireless Bridge Configuration
Examples of Deployment
WDS WLAN Services
Key Features of WDS
Deploying the WDS System
Changing the Pre-shared Key in a WDS WLAN Service

About WDS

The Wireless Distribution System (WDS) enable you to expand the wireless network by interconnecting the wireless APs through wireless links in addition to the traditional method of interconnecting APs via a wired network.

A WDS deployment is ideally suited for locations, where installing Ethernet cabling is too expensive, or physically impossible.

The WDS can be deployed in three configurations:

- Simple WDS Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration

Simple WDS Configuration

In a typical WDS configuration, the wireless APs are connected to the distribution system via an Ethernet network, which provides connectivity to the wireless controller.

However, when an AP is installed in a remote location and can't be wired to the distribution system, an intermediate AP is connected to the distribution system via the Ethernet link. This intermediate AP forwards and receives the user traffic from the remote AP over a radio link.

The intermediate AP that is connected to the distribution system via the Ethernet network is called Root AP, and the AP that is remotely located is called the Satellite AP.

The following figure illustrates the Simple WDS configuration:

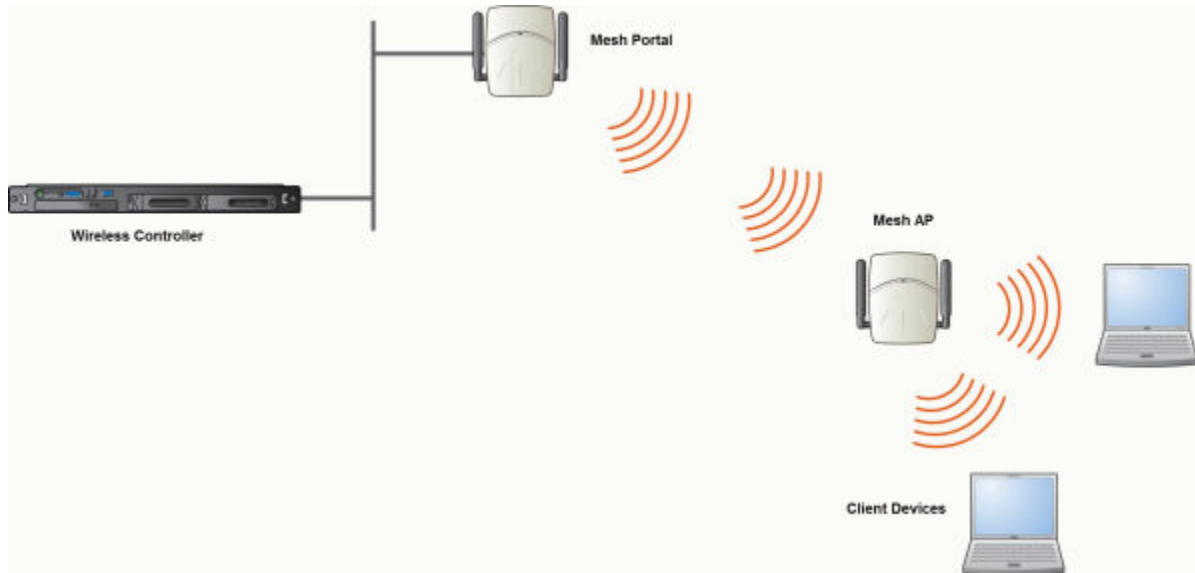


Figure 118: Simple WDS Configuration

Wireless Repeater Configuration

In Wireless Repeater configuration, a Repeater wireless AP is installed between the Root AP and the Satellite AP. The Repeater AP relays the user traffic between the Root AP and the Satellite AP. This increases the WLAN range.

The following figure illustrates the Wireless Repeater configuration:

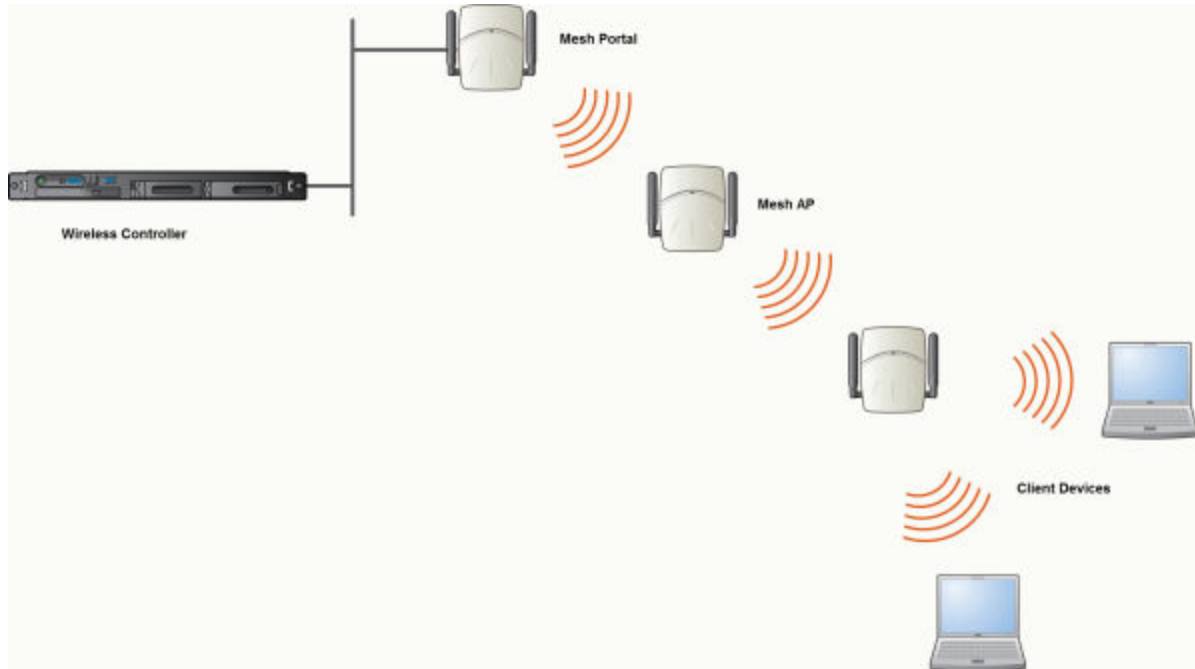


Figure 119: Wireless Repeater Configuration



Note

You should restrict the number of repeater hops in a Wireless Repeater configuration to three for optimum performance.

Wireless Bridge Configuration

In Wireless Bridge configuration, the traffic between two wireless APs that are connected to two separate wired LAN segments is bridged via WDS link. You may also install a Repeater AP between the two APs connected to two separate LAN segments.

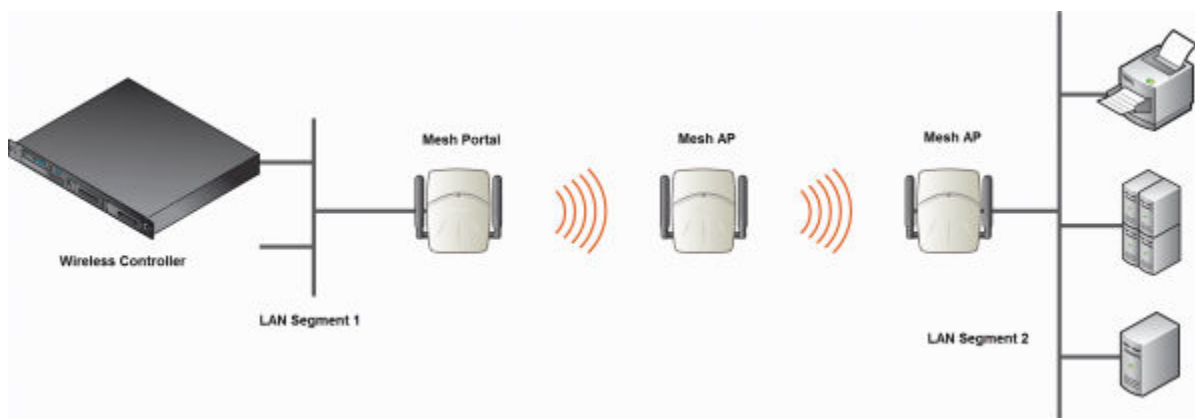


Figure 120: Wireless Bridge Configuration

When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Satellite AP is connected to the wired LAN.

Examples of Deployment

The following illustration depicts a few examples of WDS deployment.

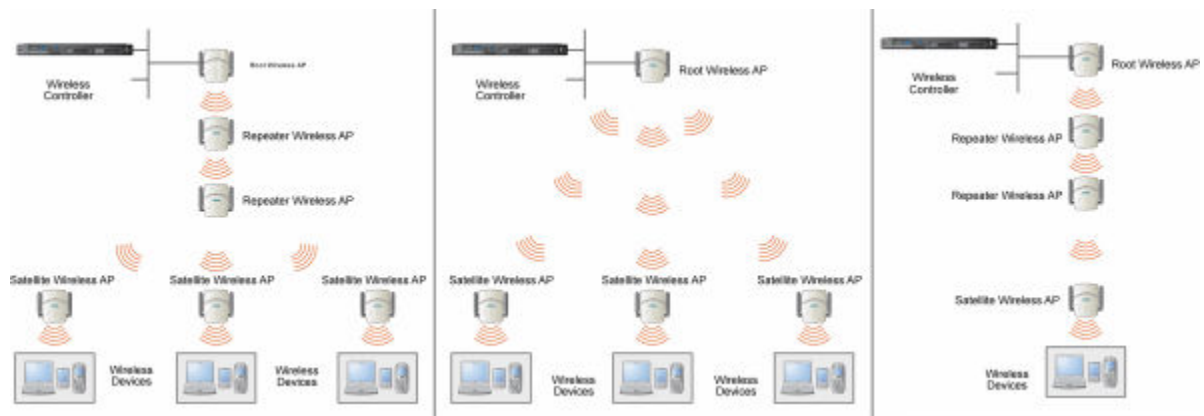


Figure 121: Examples of WDS Deployment

WDS WLAN Services

In a traditional WLAN deployment, each radio of the wireless AP can interact with the client devices on a maximum of eight networks.

In WDS deployment, one of the radios of every WDS AP establishes a WDS link on an exclusive WLAN Service. The WDS AP is therefore limited to seven network WLAN Services on the WDS radio. The other radio can interact with the client-devices on a maximum of eight WLAN Services.



Note

The root wireless AP and the Repeater APs can also be configured to interact with the client-devices. For more information, see [Assigning the Satellite Wireless APs' Radios to the Network WLAN Services](#) on page 487.

The WLAN Service on which the APs establish the WDS link is called the WDS WLAN Service.

A WDS can be setup either by using either a single WDS WLAN Service or multiple WDS WLAN Services. The following figures illustrate the point.

Figure 122 on page 475 shows:

- The rectangular enclosure denotes an office building.
- The four wireless APs — Minoru, Yosemite, Bjorn and Lancaster — are within the confines of the building and are connected to the wired network.
- The space around the office building is a ware house.
- The solid arrows point towards Preferred Parents.
- The dotted arrows point towards Backup Parents.

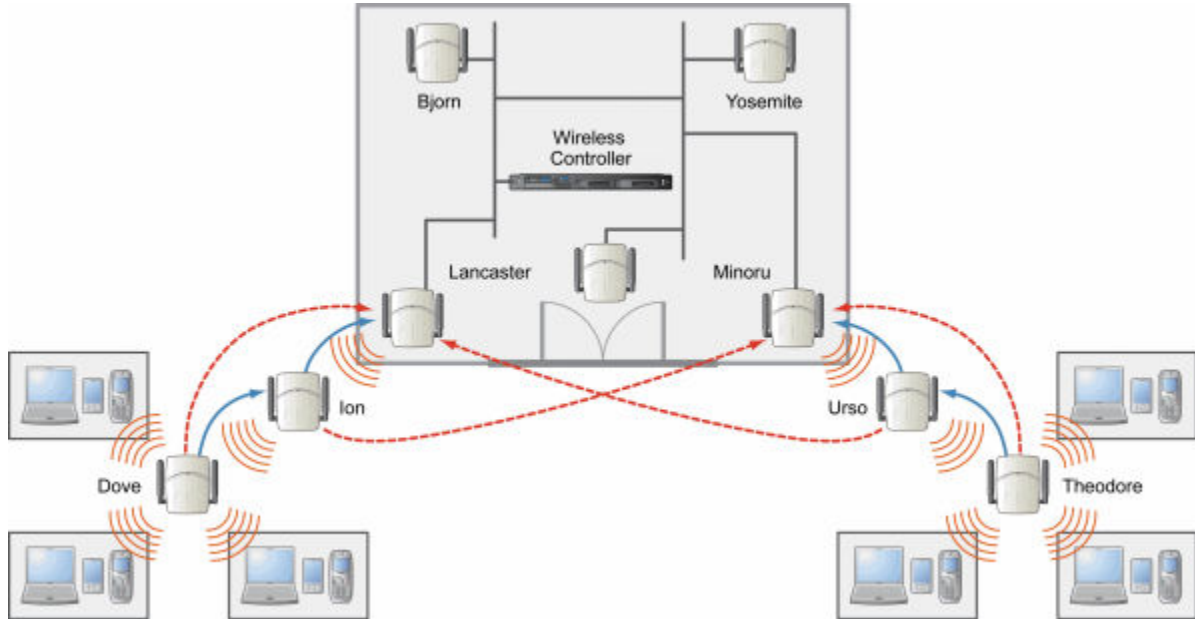


Figure 122: Deployment Example

WDS Setup with a Single WDS WLAN Service

Deploying the WDS for the above example using a single WDS WLAN Service results in the following structure.

The tree will operate as a single WDS entity. It will have a single WDS SSID and a single pre-shared key for WDS links. This tree will have multiple roots. For more information, see [Multi-Root WDS Topology](#) on page 480.

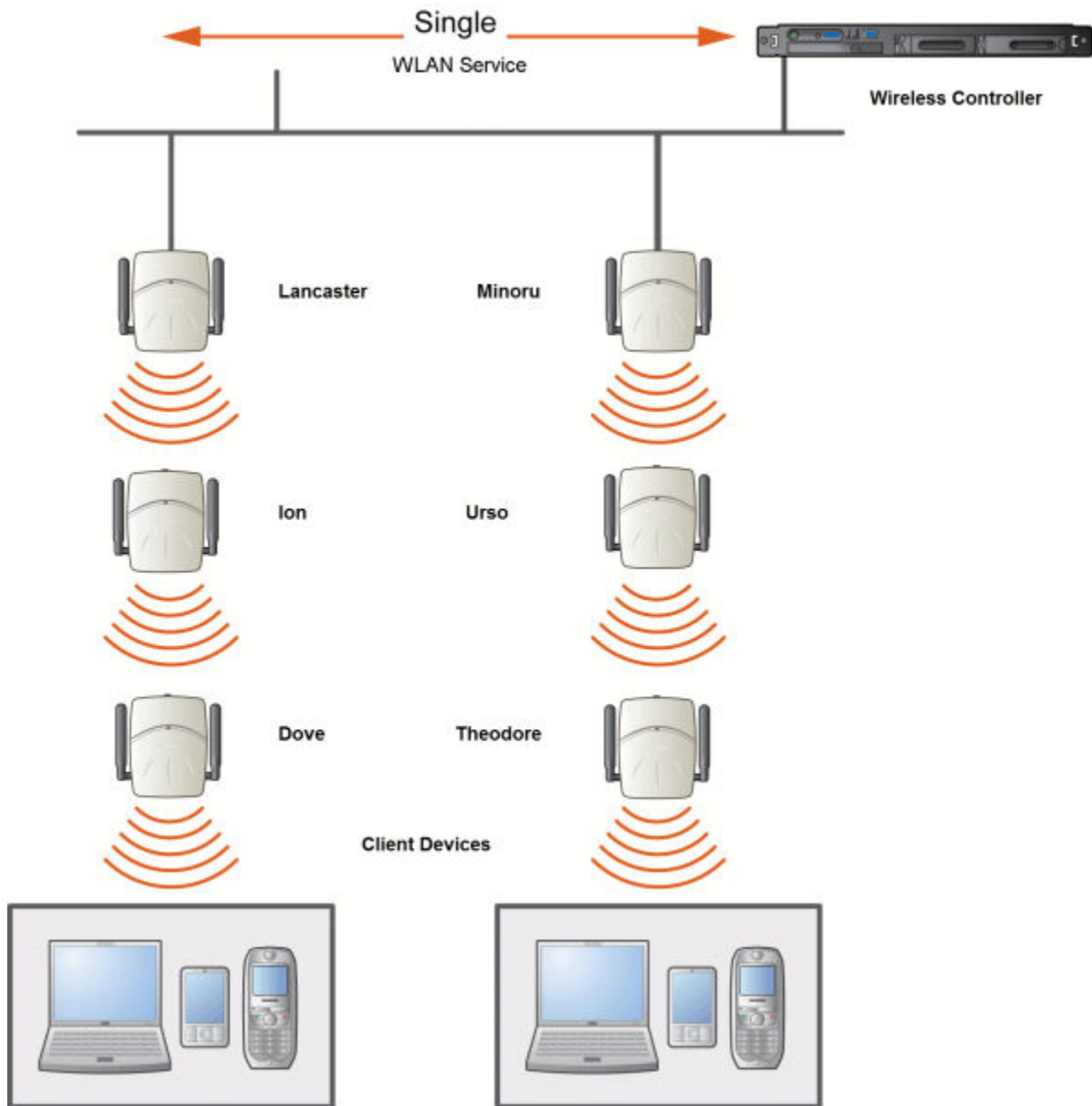


Figure 123: WDS Setup with a Single WDS WLAN Service

WDS Setup with Multiple WDS WLAN Services

You can also deploy the same WDS using two WDS WLAN Services. The Two WDS WLAN Services will create two independent WDS trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

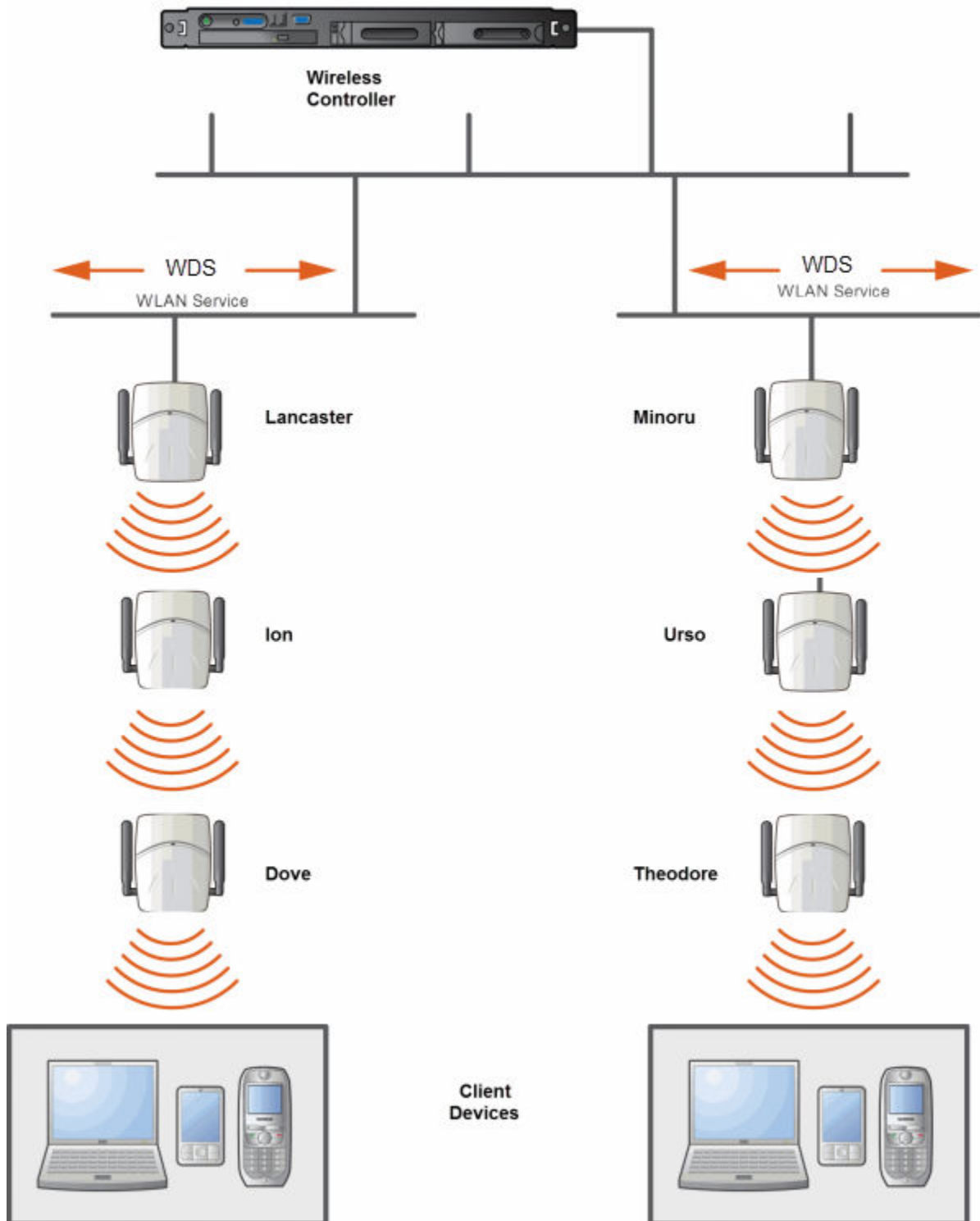


Figure 124: WDS Setup with Multiple WDS WLAN Services

Key Features of WDS

Some key features of WDS are:

- [Tree-like Topology](#) on page 478
- [Radio Channels](#) on page 480
- [Multi-Root WDS Topology](#) on page 480
- [Figure 126](#) on page 480
- [Link Security](#) on page 481

Tree-like Topology

The wireless APs in WDS configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Root AP being the tree root, and the Satellite AP being the tree leaves.

The nodes in the tree-structure have a parent-child relationship. The AP that provides the WDS service to the other APs in the downstream direction is a parent. The APs that establish a link with the AP in the upstream direction for WDS service are children.



Note

If a parent AP fails or stops to act a parent, the children APs will attempt to discover their backup parents. If the backup parents are not defined, the children APs will be left stranded.

The following figure illustrates the parent-child relationship between the nodes in a WDS topology. In [Figure 125](#) on page 479:

- Root Wireless AP is the parent of Repeater Wireless AP 1.
- Repeater Wireless AP 1 is the child of Root Wireless AP.
- Repeater Wireless AP 1 is the parent of Repeater Wireless AP 2.
- Repeater Wireless AP 2 is the child of Repeater Wireless AP 1.
- Repeater Wireless AP 2 is the parent of the following Wireless APs:
 - Satellite Wireless AP 1
 - Satellite Wireless AP 2
 - Satellite Wireless AP 3
- All the three Satellite APs are the children of Repeater Wireless AP 2.

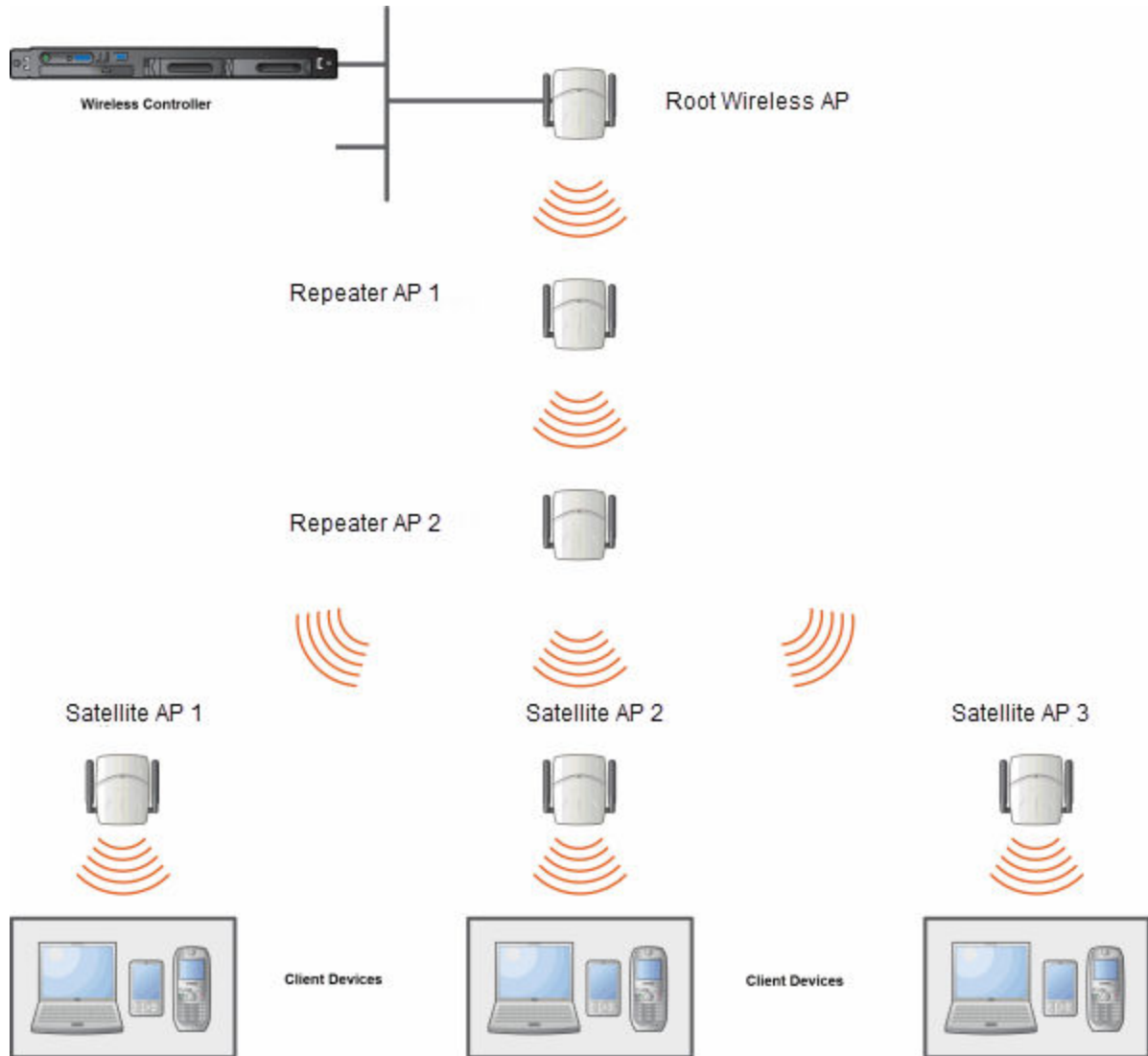


Figure 125: Parent-Child Relationship Between Wireless APs in WDS Configuration

The WDS system enables you to configure the AP's role — **parent**, **child** or **both** — from the wireless controller's interface. If the WDS AP will be serving as a parent and a child in a given topology, its role is configured as both.



Note

It is recommended that you limit the number of APs participating in a WDS tree to 8. This limit guarantees decent performance in most typical situations.



Note

If an AP is configured to serve as a scanner in Radar, it cannot be used in a WDS tree. For more information, see [Working with ExtremeWireless Radar](#) on page 517.

Radio Channels

The radio channel on which the child AP operates is determined by the parent AP.

An AP may connect to its parent AP and children APs on the same radio, or on different radios. Similarly, an AP can have two children operating on two different radios.



Note

When an AP is connecting to its parent AP and children APs on the same radio, it uses the same channel for both the connections.

Multi-Root WDS Topology

A WDS topology can have multiple Root wireless APs. [Figure 126](#) illustrates the multiple-root WDS topology.

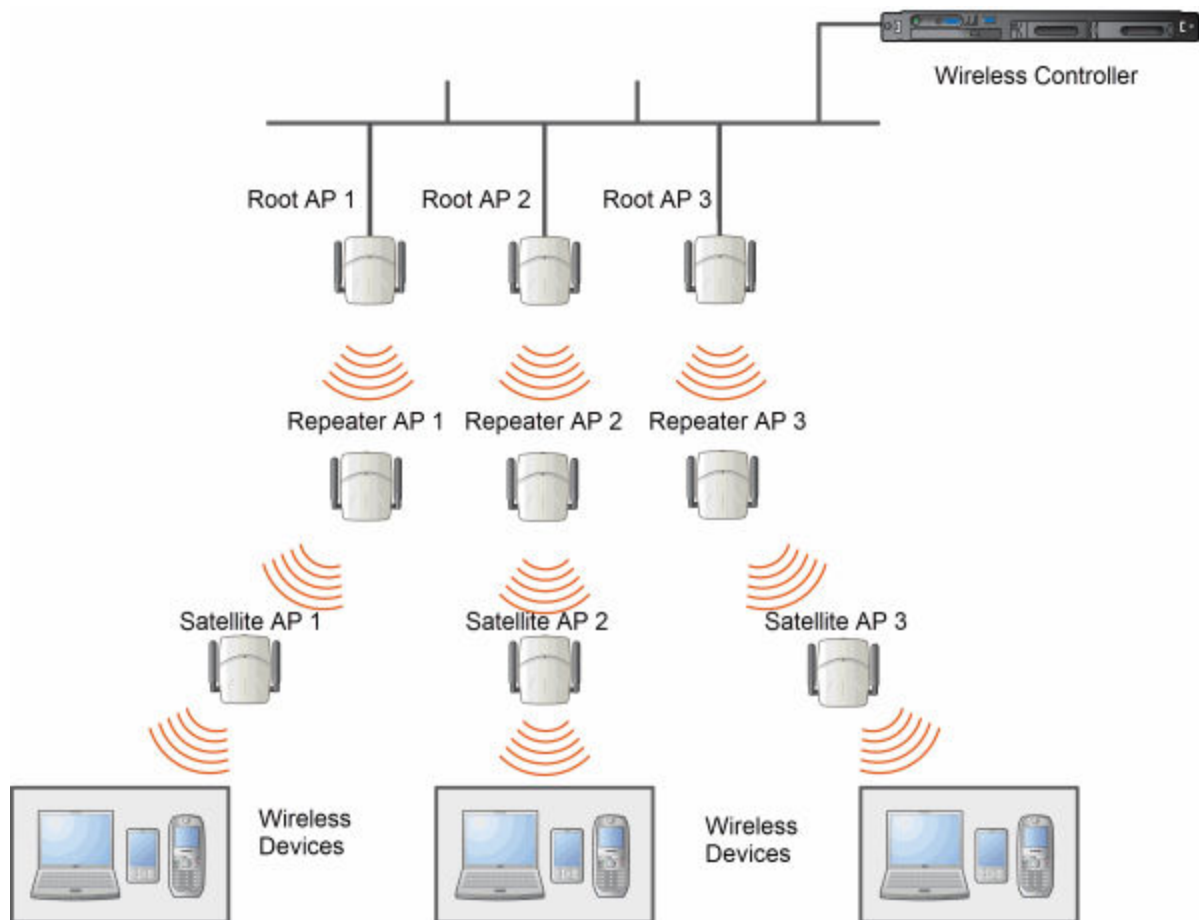


Figure 126: Multiple-root WDS Topology

Automatic Discovery of Parent and Backup Parent Wireless APs

The children wireless APs, including the Repeater wireless AP and the Satellite wireless APs, scan for their respective parents at a startup.

You can manually configure a parent and backup parent for the children APs or you can enable the children APs to automatically select the best parent out of all of the available APs. If you choose automatic parent AP selection, a child AP selects a parent AP based on its received signal strength and the number of hops to the root AP. After a parent AP and backup parent AP is selected, the wireless controller will first try to negotiate a WDS link with the parent wireless controller. If the WDS link negotiation is unsuccessful, the wireless controller will try to negotiate a link with the backup parent.

Link Security

The WDS link is encrypted using Advance Encryption Standard (AES).



Note

The keys for AES are configured prior to deploying the Repeater or Satellite APs.

Deploying the WDS System

Before you start configuring the WDS wireless APs, you must ensure the following:

- The wireless APs that are part of the wired WLAN are connected to the wired network.
- The wired wireless APs that will serve as the Root AP/Root APs of the proposed WDS topology are operating normally.
- The WLAN is operating normally.

Planning the WDS Topology

You may sketch the proposed WLAN topology on paper before you start the WDS deployment process. You should clearly identify the following in the sketch:

- WDS wireless APs with their names
- Parent-child relationships between wireless APs
- Radios that you will choose to link the wireless APs' parents and children

Provisioning the WDS APs

This step is of crucial importance and involves connecting the WDS wireless APs to the enterprise network via the Ethernet link. This is done to enable the WDS APs to connect to the wireless AP controller so that they can derive their WDS configuration.

The WDS AP's configuration includes pre-shared key, its role, preferred parent name and the backup parent name.



Note

The provisioning of WDS APs must be done before they are deployed at the target location. If the APs are not provisioned, they will not work at their target location.

WDS Deployment Overview

The following is the high-level overview of the WDS deployment process:

- 1 Connecting the WDS wireless APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the wireless controller. For more information, see [Discovery and Registration](#) on page 119.
- 2 Disconnecting the WDS APs from the enterprise network after they have discovered and registered with the wireless controller.
- 3 Creating a WDS VNS.
- 4 Assigning roles, parents and backup parents to the WDS APs.
- 5 Assigning the Satellite APs' radios to the network VNSs.
- 6 Connecting the WDS APs to the enterprise network via the Ethernet link for provisioning. For more information, see [Provisioning the WDS APs](#) on page 481.
- 7 Disconnecting the WDS APs from the enterprise network and moving them to the target location.

Note



During the WDS deployment process, the WDS APs are connected to the enterprise network on two occasions — first to enable them to discover and register with the wireless controller, and then the second time to enable them to obtain the provisioning from the wireless controller.

Connecting the WDS Wireless APs to the Enterprise Network for Discovery and Registration

Connect each WDS wireless AP to the enterprise network to enable it to discover and register itself with the wireless controller.

Note



Before you connect the WDS APs to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the wireless controller is defined according to your security needs. The **Security mode** property dictates how the wireless controller behaves when registering new and unknown devices. For more information, see [Wireless AP Registration](#) on page 121. If the **Security mode** is set to **Allow only approved APs to connect** (this is also known as secure mode), you must manually approve the WDS APs after they are connected to the network for the discovery and registration. For more information, see [New Button -- Adding and Registering a Wireless AP](#) on page 128.

Depending upon the number of Ethernet ports available, you may connect one or more WDS APs at a time, or you may connect all of them together.

Once a WDS AP has discovered and registered itself with the wireless controller, disconnect it from the enterprise network.

Configuring the WDS Wireless APs Through the Wireless Controller



Note

You must identify and mark the Preferred Parents, Backup Parents and the Child APs in the proposed WDS topology before starting the configuration process.

Configuring the WDS wireless APs involves the following steps:

- Creating a WDS WLAN Service.
- Defining the SSID name and the pre-shared key.
- Assigning roles, parents and backup parents to the WDS APs.

For ease of understanding, the WDS configuration process is explained with an example. The following figure depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four APs — Ardal, Arthur, Athens and Auberon — are within the confines of the building, and are connected to the wired network.
- The space around the building is the warehouse.
- The solid arrows point toward Preferred Parents.
- The dotted arrows point toward Backup Parents.

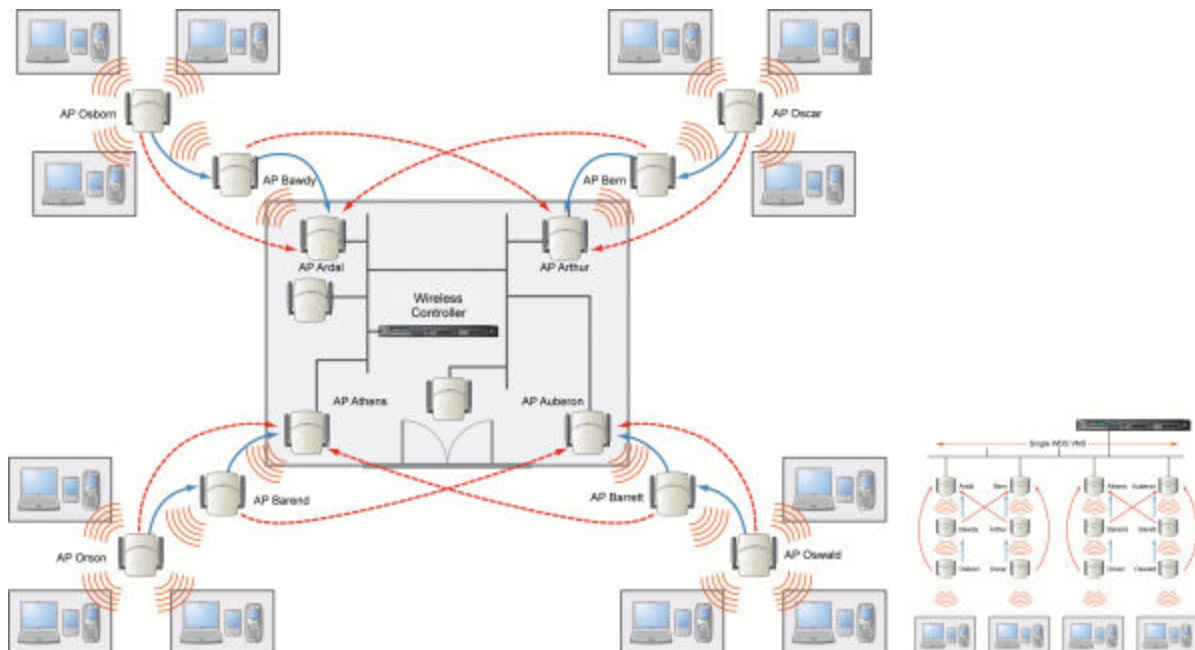


Figure 127: WDS Deployment



Note

With the single WDS VNS, the tree structure for the WDS deployment will be as depicted on the bottom right of the figure above. You can also implement the same deployment using four WDS VNSs, each for a set of APs in the four corners of the building. Each set of APs will form an isolated topology and will operate using a separate SSID and a separate Pre-shared key. For more information, see [Figure 121](#) on page 474.

To configure the WDS wireless APs through the wireless controller:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **WLAN Services** pane and select a WDS service to edit or click the **New** button.
- 3 Enter a name for the service in the **Name** field.
- 4 The **SSID** field is automatically filled in with the name, but you can change it if desired.
- 5 For **Service Type**, select **WDS**.

The screenshot shows the VNS (Virtual Network Services) interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A Logout link is visible in the top right. The left sidebar contains a tree view with categories: New..., Global, Sites, Virtual Networks, and WLAN Services (selected). Under WLAN Services, a list of service IDs is shown, including CNL-422-0-0 through CNL-422-WDS. The main content area is titled 'WLAN:' and 'WLAN Services'. It features a 'Core' section with a 'Name' field containing 'Test', a 'Service Type' section with radio buttons for Standard, WDS (selected), Mesh, Third Party AP, and Remote, and an 'SSID' field containing 'Test'. Below this is a 'Status' section with an 'Enable' checkbox checked. A 'Save' button is located at the bottom right of the form.

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

The **WLAN configuration** window displays again to show additional configuration fields.

WLAN: Ins

WLAN Services

Core

Name:

Service Type: WDS

SSID:

Suppress SSID

WDS Pre-shared key:

Status

Enable:

Wireless APs services

AP Name	Radio 1	Mode	Radio 2	Mode	WDS bridge
1523D10051090000	none	off	none	b/g	<input type="checkbox"/>
AP3715i_12b2694650000000	none	a/n	none	b/g	<input type="checkbox"/>
AP3912i_1637Y-1003100000	none	a/n/ac	none	g/n	<input type="checkbox"/>
*AP3965i_1541D10030140001	N/A	a/n/ac	N/A	b/g/n	<input type="checkbox"/>

* AP is configured as scanner
Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.

New Delete Save

- 7 To improve security for WDS links and reduce inadvertent user associations to WDS SSID, check the **Suppress SSID** checkbox. (This option is available after you save the WDS type WLANs.)

When this option is checked:

- The SSID name is not included in the SSID IE field.
- The child AP inspects the beacon for proprietary information that identifies the service.

- 8 In the **WDS Pre-shared Key** box, type the key.



Note

The pre-shared key must be 8 to 63 characters long. The WDS APs use this pre-shared key to establish a WDS link between them.



Note

Changing the pre-shared key after the WDS is deployed can be a lengthy process. For more information, see [Changing the Pre-shared Key in a WDS WLAN Service](#) on page 489.

- 9 Assign the roles, preferred parents and backup parents to the AP Radios.



Note

The roles — parent, child, and both — are assigned to the Radios of the APs. An AP may connect to its parent wireless AP and children APs on the same Radio, or on a different Radio. Similarly, a AP can have two children operating on two different Radios. The Radio on which the child AP operates is determined by the parent AP. If the AP will be serving both as parent and child, you must select both as its role.

- 10 To configure the WDS with a single WDS VNS, you must assign the roles, preferred parents and backup parents to the APs according to [the following table](#).

Table 97: Wireless APs and Their Roles

ExtremeWireless AP	Radio b/g	Radio a	Preferred Parent	Backup Parent
Ardal	Parent	Parent	See the note below.	See the note below.
Arthur	Parent	Parent	See the note below.	See the note below.
Athens	Parent	Parent	See the note below.	See the note below.
Auberon	Parent	Parent	See the note below.	See the note below.
Bawdy	Both	Child	Ardal	Arthur
Bern	Both	Child	Arthur	Ardal
Barend	Both	Child	Athens	Auberon
Barett	Both	Child	Auberon	Athens
Osborn	Child	Child	Bawdy	Ardal
Oscar	Child	Child	Bern	Arthur
Orson	Child	Child	Barend	Athens
Oswald	Child	Child	Barett	Auberon



Note

Since the Root APs — Ardal, Arthur, Athens and Auberon — are the highest entities in the tree structure, they do not have parents. Therefore, the Preferred Parent and Backup Parent drop-down lists of the Root APs do not display any AP. You must leave these two fields blank.



Note

You must first assign the 'parent' role to the APs that will serve as the parents. Unless this is done, the Parent APs will not be displayed in the Preferred Parent and Backup Parent drop-down lists of other APs.



Note

The WDS Bridge feature on the user interface relates to WDS Bridge configuration. When you are configuring the WDS Bridge topology, you must select WDS Bridge for Satellite AP that is connected to the wired network. For more information, see [Wireless Bridge Configuration](#) on page 473.

- 11 To assign the roles, preferred parent and backup parent:
 - a From the radio **b/g** drop-down list of the Root APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
 - b From the radio **a** drop-down list of the Root APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
 - c From the radio **a** and radio **b/g** drop-down list of other APs, click the roles according to [Table 97](#) on page 486.
 - d From the **Preferred Parent** drop-down list of other APs, click the parents according to [Table 97](#) on page 486.
 - e From the **Backup Parent** drop-down list of other APs, click the backup parents according to [Table 97](#) on page 486.

Wireless APs services						
AP Name	Radio 1	Mode	Radio 2	Mode	Preferred Parent	Backup Parent
Ardal	parent	a	parent	b/g		
Arthur	parent	a	parent	b/g		
Athens	parent	a	parent	b/g		
Auberon	parent	a	parent	b/g		
Bawdy	both	a	child	b/g		
Bern	both	a	child	b/g		
Barend	both	a	child	b/g		
Barett	both	a	child	b/g		
Osborn	child	a	child	b/g		
Oscar	child	a	child	b/g		
Orson	child	a	child	b/g		
Oswald	child	a	child	b/g		

- 12 Click **Save** to save your changes.

Assigning the Satellite Wireless APs' Radios to the Network WLAN Services

You must assign the Satellite wireless APs' radios to the network WLAN Services.



Note

Network WLAN Services are the typical WLAN Services on which the APs service the client devices: Routed, Bridge Traffic Locally at EWC, and Bridge Traffic Locally at AP. For more information, see [VNS Global Settings](#) on page 345.

To Assign the Satellite wireless APs' Radios to the Network WLAN Service:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- In the left pane, expand the **WLAN Services** pane and select a network WDS service to edit

Wireless APs:Select APs:

	Radio 1	Radio 2	AP Name
<input type="checkbox"/>	a	<input type="checkbox"/> b/g	Arthur
<input type="checkbox"/>	a	<input type="checkbox"/> b/g	Athens
<input type="checkbox"/>	a	<input type="checkbox"/> b/g	Auberon
<input type="checkbox"/>	a	<input type="checkbox"/> b/g	Barett
<input type="checkbox"/>	a	<input type="checkbox"/> b/g	Bawdy
<input checked="" type="checkbox"/>	a	<input checked="" type="checkbox"/> b/g	Orson
<input checked="" type="checkbox"/>	a	<input checked="" type="checkbox"/> b/g	Osborn
<input checked="" type="checkbox"/>	a	<input checked="" type="checkbox"/> b/g	Oscar
<input checked="" type="checkbox"/>	a	<input checked="" type="checkbox"/> b/g	Oswald

- In the **Wireless APs** list, select the radios of the Satellite APs — Osborn, Oscar, Orson and Oswald.

**Note**

If you want the Root AP and the Repeater APs to service the client devices, you must select their radios in addition to the radios of the Satellite APs.

- To save your changes, click **Save**.
- Log out from the wireless controller.

Connecting the WDS Wireless APs to the Enterprise Network for Provisioning

You must connect the WDS wireless APs to the enterprise network once more to enable them to obtain their configuration from the wireless controller. The configuration includes the pre-shared key, the AP's role, preferred parent and backup parent. For more information, see [Provisioning the WDS APs](#) on page 481.

**Warning**

If you skip this step, the WDS wireless APs will not work at their target location.

Moving the WDS Wireless APs to the Target Location

**Note**

If you change any of the following configuration parameters of a WDS AP, the WDS AP will reject the change: Reassigning the WDS AP's role from **Child** to **None**, Reassigning the WDS AP's role from **Both** to **Parent**, and changing the **Preferred Parent** of the WDS AP. However, the wireless controller will display your changes, as these changes will be saved in the database. To enable the WDS AP to obtain your changes, you must remove it from the WDS location and then connect it to the wireless Controller via the wired network.

**Note**

If you change any of the following radio properties of a WDS AP, the WDS AP will reject the change: Disabling the radio on which the WDS link is established, lowering the radio's Tx Power of a radio on which the WDS link is established, or changing the country

- 1 Disconnect the WDS wireless APs from the enterprise network, and move them to the target location.
- 2 Install the WDS APs at the target location.
- 3 Connect the APs to a power source. The discovery and registration processes are initiated.

Changing the Pre-shared Key in a WDS WLAN Service

To Change the Pre-shared Key in a WDS WLAN Service

- 1 Create a new WDS WLAN Service with a new pre-shared key.
- 2 Assign the RF of the APs from the old WDS to the new WDS WLAN Service.
- 3 Check the **WDS AP Statistics** report page to ensure that all the WDS APs have connected to the wireless controller via the new WDS VNS. For more information, see [Viewing Statistics for APs](#) on page 572.
- 4 Delete the old WDS WLAN Service. For more information, see [Deleting a VNS](#) on page 438.

13 Availability and Session Availability

Availability
Session Availability
Viewing SLP Activity

Availability

The Extreme Networks ExtremeWireless Software system provides the availability feature to maintain service availability in the event of a controller outage.



Note

During the failover event, the maximum number of failover APs the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform.

Wireless APs that attempt to connect to the secondary controller during a failover event are assigned to the WLAN Service that is defined in the system's default AP configuration, provided the administrator has not assigned the failover APs to one or more VNSs. If a system default AP configuration does not exist for the controller (and the administrator has not assigned the failover APs to any WLAN Service), the APs will not be assigned to any WLAN Service during the failover.

A controller will not accept a connection by a foreign AP if the controller believes its availability partner controller is in service. Also, the default AP configuration assignment is only applicable to new APs that failover to the backup controller. Any AP that has previously failed over and is already known to the backup system will receive the configuration already present on that system. For more information, see [Configuring the Default Wireless AP Settings](#) on page 130.

During the failover event when the AP connects to the secondary controller, the users are disassociated from the AP. Consequently, the users must log on again and be authenticated on the secondary controller before the wireless service is restored.



Note

If you want the mobile user's session to be maintained, you must use the 'session availability' feature that enables the primary controller's APs to failover to the secondary controller fast enough to maintain the session availability (user session). For more information, see [Session Availability](#) on page 498.

The availability feature provides APs with a list of local active interfaces for the active controller as well as the active interfaces for the backup controller. The list is sorted by top-down priority.

If the connection with an active controller link is lost (poll failure), the AP automatically scans (pings) all addresses in its availability interface list. The AP then connects to the highest priority interface that responds to its probe.

Events and Actions in Availability

If one of the controllers in a pair fails, the communication between the two controllers stops. This triggers a failover condition and a critical message is displayed in the information log of the secondary controller.

Timestamp	Type	Component	Log Message
02/28/14 06:18:35	Critical	CLI	USER GENERATED EVENT: Critical Logs During Smoke Test - lab-422-g-1402280325
02/28/14 04:12:39	Critical	CLI	USER GENERATED EVENT: Critical Logs During Smoke Test - lab-422-g-1402280325

2 messages [1 to 2]

First Previous 1 Next Last Tech Support Export Refresh

After an AP on the failed controller loses its connection, it will try to connect to all enabled interfaces on both controllers without rebooting. If the AP is not successful, it will begin the discovery process. If the AP is not successful in connecting to the controller after five minutes of attempting, the AP will reboot if there is no **Bridge traffic locally at the AP** topology associated to it.

All mobile user's sessions using the failover AP will terminate except those associated to a **Bridge traffic locally at the AP** and if the **Maintain client sessions in event of poll failure** option is enabled on the **AP Properties** tab or **AP Default Settings** screen.

When the APs connect to the second controller, they are either assigned to the VNS that is defined in the system's default AP configuration or manually configured by the administrator. The mobile users log on again and are authenticated on the second controller.

When the failed controller recovers, each controller in the pair goes back to normal mode. They exchange information including the latest lists of registered APs. The administrator must release the APs manually on the second controller, so that they may re-register with their home controller. Foreign APs can now all be released at once by using the **Approve as Foreign** button on the **Access Approval** screen to select all foreign APs, and then clicking **Release**.

To support the availability feature during a failover event, you need to do the following:

- 1 Monitor the critical messages for the failover mode message, in the information log of the remaining controller (in the **Logs & Traces** section of the Wireless Assistant).
- 2 After recovery, on the controller that did not fail, select the foreign APs, and then click **Release** on the **Access Approval** screen.

Availability Prerequisites

Before you configure availability, you must do the following:

- Choose the primary and secondary controllers.
- Verify the network accessibility for the UDP connection between the two controllers. The availability link is established as a UDP session on port 13911.
- Set up a server for AP subnets to support Option 78 for SLP, so that it points to the IP addresses of the physical interfaces on both the controllers.
- Ensure that the Poll Timeout value on the **AP Properties** tab **Advanced** dialog is set to 1.5 to 2 times of **Detect link failure** value on the **Controller > Availability** screen. For more information, see [AP Properties Tab - Advanced Settings](#) on page 154.

If the Poll Timeout value is more than 1.5 to 2 times of Detect link failure value, the APs failover will be unnecessarily delayed, because the APs will continue polling the primary controller even though the secondary controller is ready to accept them as the failover APs.

- To achieve ideal availability behavior, set the Poll Timeout value for all APs to 15 seconds, and the Detect link failure on the **Controller > Availability** screen to 10 seconds.

Configuring Availability Using the Availability Wizard

The availability wizard allows you to create an availability pair from one of the controllers that will be in the availability pair. When creating the availability pair, you also have the option to synchronize VNS definitions and GuestPortal user accounts between the paired controllers.

To Configure Availability Using the Availability Wizard:

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

- In the **Availability Wizard** section, click **Start**.
The **Availability Pair Wizard** screen displays.

- In the **Connection Details** section, do the following:
 - **Select Port** — Select the port and IP address of the primary controller that is to be used to establish the availability link.
 - **Peer Controller IP** — Type the IP address of the peer (secondary) controller.
 - **User** — Type the login user name credentials of an account that has full administrative privileges on the peer controller.
 - **Password** — Type the login password used with the user ID to login to the peer controller.
 - **Enable Fast Failover** — Select this checkbox to enable Fast Failover for the availability pair.
- In the **Synchronize Options** section, do the following:



Note

Synchronizing the VNS definitions will delete and replace existing VNS definitions on the peer controller.

- **Synchronize Guest Portal Accounts** — Select this checkbox to push GuestPortal user accounts to the peer controller.
- Click **Next**.

- 7 If you are synchronizing topology definitions, the **Topology Definitions** screen displays. Do the following:
 - a In the Synchronization Settings section, complete the topology properties that are missing. Any topology that did not already exist on the peer controller will have missing properties on the **Topology Definitions** screen.
 The fields configured are actual parameter values that are configured at the remote Controller with respect to associated topologies chosen for synchronization. Some of these parameters are: Interface IP address, Netmask, L2 port, VLAN ID, range, etc.
 - b Click **Finish**.
- 8 If you are not synchronizing topology definitions, the availability wizard completes the configuration.
- 9 Click **Close**.

This operation marks the desired topologies for synchronization. The two controllers exchange information and the configuration is applied to the remote controller.

On the local controller, the “Enable Synchronization of System Configuration” becomes selected. This can be double checked by navigating to **VNS > Global > Sync Summary**. This tab also lists all topologies, roles, WLAN Services and VNSes with their synchronization status (on or off).

The Sync status for any of these elements can also be changed from this tab.

All these configurable elements have a Synchronize check box (on their main/general configuration tab) that allows for individual control and selection of availability from the main element configuration page.

Configuring Availability Manually

When configuring availability manually, you configure each controller separately.

- 1 On the wireless controller **Availability** screen, set up the controller in **Paired Mode**.
- 2 On the **VNS configuration** window, define a VNS (through topology, WLAN service, role and VNS configuration) on each controller with the same SSID. The IP addresses must be unique. For more information, see [Manually Creating a VNS](#) on page 374. A controller VLAN Bridged topology can permit two controllers to share the same subnet. This setup provides support for mobility users in a VLAN Bridged VNS.
- 3 On both controllers, on the AP Registration screen, select the Security Mode **Allow only approved APs to connect** option so that no more APs can register unless they are approved by the administrator.
- 4 On each controller, on the AP configuration **Access Approval** screen, check the status of the APs and approve any APs that should be connected to that controller.

System AP defaults can be used to assign a group of VNSs to the foreign APs:

- If the APs are not yet known to the system, the AP will be initially configured according to AP default settings. To ensure better transition in availability, Extreme Networks recommends that the AP default settings match the desired assignment for failover APs.
- AP assignment to WLAN Services according to the AP default settings can be overwritten by manually modifying the AP assignment. (For example, select and assign each WLAN service that the AP should connect to.)
- If specific foreign APs have been assigned to a WLAN service, those specific foreign AP assignments are used.

Alternate Method to Setting Up a Wireless AP

An alternate method to setting up Wireless APs for Availability mode include:

- 1 Add each AP manually to each controller.
- 2 On the **AP Properties** screen, click **Add Wireless AP**.
- 3 Define the AP, and then click **Add Wireless AP**.

Manually defined APs will inherit the default AP configuration settings.



Caution

If two wireless controllers are paired and one has the Allow All option set for AP registration, all APs will register with that wireless controller.

Setting the Primary or Secondary Wireless Controllers for Availability

To Set the Primary or Secondary Controllers for Availability:

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

- 3 To enable availability, select the **Paired** option.
- 4 Do one of the following:
 - For a primary controller, in the **Wireless IP Address** box, type the IP address of the data interface of the secondary controller. This IP address must be on a routable subnet between the two controllers.
 - For a secondary controller, in the **Wireless IP Address** box, type the IP address of the Management port or data interface of the primary controller.

- 5 Set this controller as the primary or secondary connection point:
 - To set this controller as the primary connection point, select the **Current Wireless is primary connect point** checkbox.
 - To set this controller as the secondary connection point, clear the **Current Wireless is primary connect point** checkbox.

If the **Current Wireless is primary connect point** checkbox is selected, the specified controller sends a connection request. If the **Current Wireless is primary connect point** checkbox is cleared, the specified controller waits for a connection request. Confirm that one controller has this checkbox selected, and the second controller has this checkbox cleared, since improper configuration of this option will result in incorrect network configuration.

- 6 On both the primary and secondary controllers, type the **Detect link failure value**.



Note

Ensure that the Detect link failure value on both the controllers is identical.

- 7 On both the primary and secondary controllers, select the **Synchronize GuestPortal Guest Users** option to synchronize GuestPortal guest accounts between the controllers.
- 8 From the top menu, click **AP**.
- 9 In the left pane, click **Global Settings > AP Registration**. To set the **security mode** for the controller, select one of the following options:
 - **Allow all wireless APs to connect** — If the controller does not recognize the serial number, it sends a default configuration to the AP. Or, if the controller recognizes the serial number, it sends the specific configuration (port and binding key) set for that AP.
 - **Allow only approved wireless APs to connect** — If the controller does not recognize the serial number, the APs will be in pending mode and the administrator must manually approve them. Or, if the controller recognizes the serial number, it sends the configuration for that AP.



Note

During the initial setup of the network, it is recommended 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, it is recommended 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 147.

- 10 To save your changes, click Save.



Note

When two controllers have been paired as described above, each controller's registered APs will appear as foreign on the other controller in the list of available APs when configuring a VNS topology.

- 11 Verify that availability is configured correctly.

Verifying Availability

To verify that availability is configured correctly:

- From the top menu of either of the two controllers, click **Reports**.

The screenshot shows a navigation menu with the following items: Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The 'Reports' menu is expanded, showing a list of available reports:

- Active APs
- Wired Ethernet Statistics
- Wireless Statistics
- Admission Control Statistics
- Mesh Statistics
- Wireless Load Groups
- AP Availability
- AP Inventory
- Nearby AP
- AP Performance by Radio
- AP Performance by SSID and Radio
- AP Accessibility

Other menu items visible include: APs, Clients, Filter Statistics, Topology, Mobility, Radar, Controller Status, Routing Protocols, and RADIUS.

- From the **Reports and Displays** menu, click **AP Availability**. The Wireless Availability Report is displayed.

The screenshot shows the 'lab-422-g - Reports - Wireless AP Availability' page. The page title is 'lab-422-g - Reports - Wireless AP Availability'. There are radio buttons for 'No refresh' (selected) and 'Refresh every 30 secs', followed by an 'Apply' button.

The main content area displays 'Availability not configured'.

Color Legend:

- Wireless AP has active tunnel passing data (Green)
- Wireless AP has backup tunnel (Blue)
- Wireless AP not connected (Orange)
- No information (Grey)

Wireless APs List:

AP ID	MAC Address	Uptime	IP Address	Status
[Local] C4110 - ap1 - AP4102	0002000609223321	00:11:88:28:EA:74	10.219.40.10	Active tunnel passing data
[Local] C4110 - ap2 - AP3620	0500008043050317	00:1A:E8:14:10:41	10.219.40.13	Active tunnel passing data
[Local] C4110 - ap3 - AP3825e	1406000708420000	20:B3:99:AE:C6:06		Not connected

Additional information: uptime: 11:11:33 for AP4102, uptime: 10:33:11 for AP3620, and uptime: N/A for AP3825e.

Data as of Feb 28, 2014 03:29:06 pm

Buttons: Refresh, Close

- 3 Check the statement at the top of the screen.

If the statement reads **Availability link is up**, the availability feature is configured correctly. If the statement reads **Availability link is down**, check the configuration error logs. For more information on logs, see the Extreme Networks ExtremeWireless *Maintenance Guide*.

Session Availability

Session availability enables wireless APs to switch over to a standby (secondary) wireless controller fast enough to maintain the mobile user's session availability in the following scenarios:

- The primary wireless controller fails (see [Figure 128](#)).

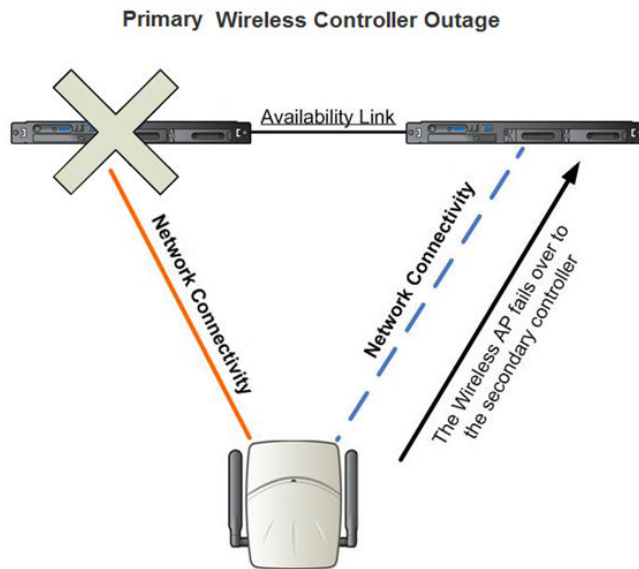


Figure 128: AP Fail Over When Primary Controller Fails

- The wireless AP's network connectivity to the primary controller fails (see [Figure 129](#)).

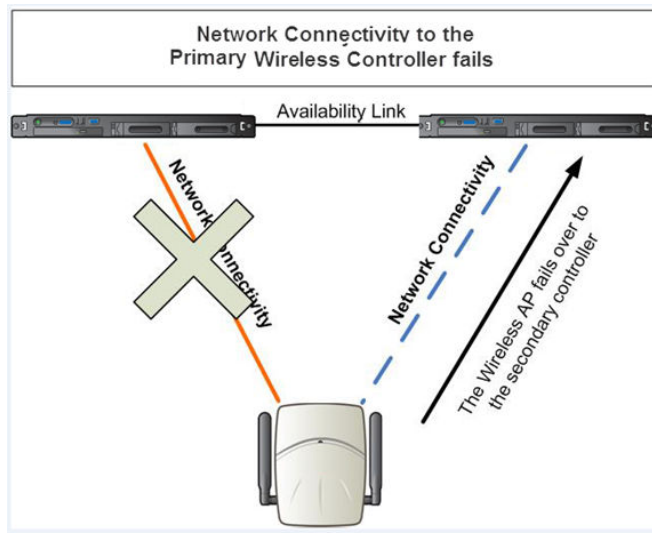


Figure 129: AP Fail Over When Connectivity to Primary Fails

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

In session availability mode (Figure 130), the APs connect to both the primary and secondary controllers. While the connectivity to the primary controller is via the “active” tunnel, the connectivity to the secondary controller is via the “backup” tunnel.

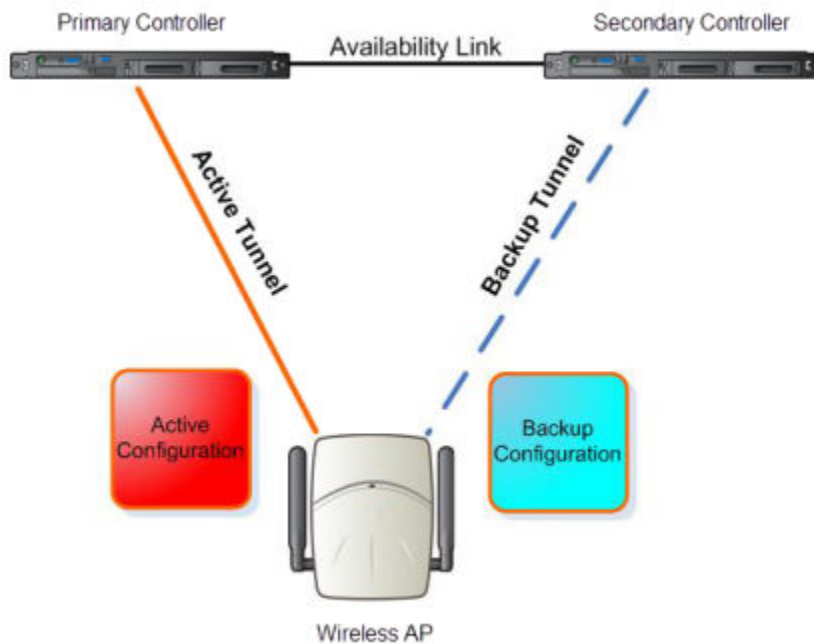


Figure 130: Session Availability Mode

The following is the traffic flow of the topology illustrated in Figure 130:

- The AP establishes the active tunnel to connect to the primary controller.
- The controller sends the configuration to the AP. This configuration also contains the port information of the secondary controller.
- On the basis of the secondary controller’s port information, the AP connects to the secondary controller via the backup tunnel.
- After the connection is established via the backup tunnel, the secondary controller sends the backup configuration to the wireless AP.
- The AP receives the backup configuration and stores it in its memory to use it for failing over to the secondary controller. All this while, the AP is connected to the primary controller via the ‘active’ tunnel.

Session availability applies only to the following topologies:

- Bridge Traffic Locally at Controller
- Bridge Traffic Locally at AP

Events and Actions in Session Availability

In the event of a primary controller outage, or the network connectivity failure to the primary controller, the wireless AP:

- Sends a 'tunnel-active-req' request message to the secondary controller.
- The secondary controller accepts the request by sending the 'tunnel-activate-response' message.
- The AP applies the backup configuration and starts sending the data. The client devices' authentication state is not preserved during failover.

When the fast failover takes place, a critical message is displayed in the information log of the secondary controller.



Note

In session availability, the maximum number of failover APs that the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform.

When the failed controller recovers, each controller in the pair goes back to normal mode. They exchange information that includes the latest lists of registered APs. The administrator must release the APs manually on the second controller, so that they may re-register with their home controller. Foreign APs can now all be released at once by using the **Approve as Foreign** button on the **Access Approval** screen to select all foreign APs, and then clicking **Released**.

To support the availability feature during a failover event, administrators need to do the following:

- 1 Monitor the critical messages for the failover mode message, in the information log of the secondary controller (in the **Logs & Traces** section of the Wireless Assistant).
- 2 After recovery, on the secondary controller, select the foreign APs, and then click **Release** on the **Access Approval** screen.

After the APs are released, they establish the active tunnel to their home controller and backup tunnel to the secondary controller.

Enabling Session Availability

Session availability is supported when fast failover is enabled and when "Synchronize System Configuration" is selected. For more information, see [Configuring Fast Failover and Enabling Session Availability](#) on page 501.

In session availability, mobile user devices are able to retain their IP address. In addition, the mobile user device does not have to re-associate after the failover. These characteristics ensure that the failover is achieved within 5 seconds, which is fast enough to maintain the mobile user's session.



Note

In session availability, the fast failover is achieved within 5 seconds only if there is at least one client device (mobile unit) associated to the AP. In the absence of any client device, the AP takes more time to failover since there is no need to preserve the user session.

The authentication state is not preserved during fast failover. If a WLAN Service requires authentication, the client device must re-authenticate. However, in such a case, the session availability is not guaranteed because authentication may require additional time during which the user session may be disrupted.

Session availability is not supported in a WLAN Service that uses Captive Portal (CP) authentication.

Session availability does not support user-specific filters as these filters are not shared between the primary and secondary controller.

Configuring Fast Failover and Enabling Session Availability

Before you configure the fast failover feature, ensure the following:

- The primary and secondary controllers are properly configured in availability mode. For more information, see [Availability](#) on page 490.
- The pair of controllers in availability mode is formed by one of the following combinations:
 - C5110 and C5110
 - C5210 and C5210
 - C4110 and C4110
 - C5110 and C4110
 - V2110 and V2110 (Using the same V2110 profile, two V2110 Small, or two V2110 Medium, or two V2110 Large.)
 - C25 and C25
 - C35 and C35
- Both the primary and secondary controllers are running the most recent Extreme Networks ExtremeWireless software.
- A network connection exists between the two controllers.
- The APs are operating in availability mode.
- The deployment is designed in such a way that the service provided by the APs is not dependent on which controller the APs associate with. For example, the fast failover feature will not support the deployment in which the two controllers in availability mode are connected via a WAN link.
- Both the primary and secondary controllers have equivalent upstream access to the servers on which they depend. For example, both the controllers must have access to the same RADIUS and servers.
- The users (client devices) that use DHCP must obtain their addresses from a DHCP Server that is external to the controller.
- Time on all the network elements (both the controllers in availability pair, APs, DHCP and RADIUS servers etc.) is synchronized. For more information, see [Configuring Network Time](#) on page 88.



Note

The fast failover feature works optimally in fast networks (preferably switched networks).

To configure Fast Failover and enable Session Availability:

- 1 Log on to both the primary and secondary controllers.
- 2 From the top menu of the primary controller, click **Controller**.

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

- 4 Under **Controller Availability Settings**, select **Paired**.
- 5 Select the **Fast Failover** checkbox.
- 6 Type the appropriate value in the **Detect link failure** box.

The **Detect link failure** field specifies the period within which the system detects link failure after the link has failed. For fast failover configuration, this parameter is tied closely to the **Poll Timeout** parameter on the **AP Properties** tab **Advanced** dialog. The **Poll Timeout** field specifies the period for which the wireless AP waits before re-attempting to establish a link when its polling to the primary controller fails.

For the fast failover feature to work within 5 seconds, the **Poll Timeout** value should be 1.5 to 2 times the **Detect link failure** value. For example, if you have set the **Detect link failure** value to 2 seconds, the **Poll Timeout** value should be set to 3 or 4 seconds.

- 7 In the **Synchronization Option** area, select **Synchronize System Configuration**.

This is a global parameter that enables synchronization of VNS configuration components (topology, role, WLAN Service, VNS) on both controllers paired for availability and/or fast failover.

For more information about synchronization, see [Using the Sync Summary](#) on page 365.

- 8 Click **Save**.

- 9 Set the APs' **Poll Timeout** value for fast failover.
 - a From the top menu of the primary controller, click **AP**.
 - b Select the checkbox for one or more APs.
 - c Click **Actions > Multi Edit**. The **Multi Edit** dialog displays.

The screenshot shows the 'Multi Edit' dialog box with the following fields and sections:

- AP Properties [Hide]**
 - Location:
 - Zone:
 - Poll Timeout [Seconds]:** (highlighted with a red box)
 - Secure Tunnel:
 - Secure Tunnel Lifetime [hours]:
 - Remote Access:
 - Location-based Service:
 - Maintain client sessions in event of poll failure:
 - Restart service without controller:
 - Use broadcast for disassociation:
 - LLDP:
 - Multicast prioritized as voice:
 - IP Multicast Assembly:
 - Balanced Channel List Power:
 - LED:
 - Country:
 - Antennas: Professional Installer
- Radio Settings [Hide]**
 - Radio 1**
 - Admin Mode:
 - Radio Mode:
 - Channel Width:
 - Radio 2**
 - Admin Mode:
 - Radio Mode:
 - Channel Width:

Buttons: **Apply** and **Close**

- d In the **Poll Timeout** field, enter the poll timeout value in seconds.
- e Click **Apply**.

Note

The fast failover configuration must be identical on both the primary and secondary ExtremeWireless Controller. Log on to the primary controller. If the configuration is not identical, see the ExtremeWireless *Maintenance Guide*.

After you have configured fast failover, you can verify session availability to preserve the user session during the failover.

Verifying Session Availability

To have session availability, you must ensure the following:

- The primary and secondary wireless controllers are properly configured in 'availability' mode. For more information, see [Availability](#) on page 490.
- The fast failover feature is properly configured. For more information, see [Configuring Fast Failover and Enabling Session Availability](#) on page 501.



Note

If you haven't configured the fast failover feature, the **Enable Session Availability** checkbox is not displayed.

- Time on all the network elements — both the wireless controllers in availability pair, APs, and RADIUS servers etc.— is synchronized. For more information, see [Configuring Network Time](#) on page 88.
- Both the wireless controllers in fast failover mode must be running the most recent wireless controller software release.
- If you are using **Bridge Traffic Locally at Controller** topology, you must select **None** from the **DHCP Option** drop-down menu.
- The **Bridge Traffic Locally at Controller** must be mapped to the same VLAN on both the primary and secondary wireless controllers.

To Verify the Session Availability Feature Is Configured Correctly:

- 1 From the top menu of either of the two controllers, click **Reports**.

The screenshot displays the network management interface. At the top, a navigation bar includes a home icon, and tabs for Home, Logs, Reports (highlighted), Controller, AP, VNS, Radar, and Help. A Logout link is visible in the top right corner. On the left, a sidebar menu lists various categories: APs, Clients, Filter Statistics, Topology, Mobility, Radar, Controller Status, Routing Protocols, and RADIUS. The APs category is expanded, showing a list of reports: Active APs, Wired Ethernet Statistics, Wireless Statistics, Admission Control Statistics, Mesh Statistics, Wireless Load Groups, AP Availability, AP Inventory, Nearby AP, AP Performance by Radio, AP Performance by SSID and Radio, and AP Accessibility. The main content area, titled 'Available AP Reports', lists the same reports in a vertical stack.

Available AP Reports	
Active APs	
Wired Ethernet Statistics	
Wireless Statistics	
Admission Control Statistics	
Mesh Statistics	
Wireless Load Groups	
AP Availability	
AP Inventory	
Nearby AP	
AP Performance by Radio	
AP Performance by SSID and Radio	
AP Accessibility	

- From the **Reports and Displays** menu, click **Wireless AP Availability**. The **Wireless Availability Report** is displayed.

EWC - Reports - Wireless AP Availability No refresh Refresh every 30 secs Apply

Availability not configured

Color Legend:

Wireless AP has active tunnel passing data	Wireless AP has backup tunnel	Wireless AP not connected	No information
--	-------------------------------	---------------------------	----------------

Wireless APs List:

[Local] 1 111111111111111111 uptime: N/A	[Local] 2 111111111111111112 uptime: N/A	[Local] 21 211111111111111111 uptime: N/A	[Local] 22 222222222222222222 uptime: N/A
[Local] 23 222222222222222223 uptime: N/A	[Local] 233 222222222222222233 uptime: N/A	[Local] 3 111111111111111113 uptime: N/A	[Local] 3801i 11111111111113801 uptime: N/A
[Local] 3805i 11111111111113805 uptime: N/A	[Local] 3825e 11111111111113825 uptime: N/A	[Local] 4 1111111111111114 uptime: N/A	[Local] 5 1111111111111115 uptime: N/A

Data as of Jun 16, 2015 08:15:53 am Refresh Close

- Check the statement at the top of the screen.
If the statement reads Availability link is up, the availability feature is configured correctly. If the statement reads Availability link is down, check the configuration error in logs. For more information on logs, see the Extreme Networks ExtremeWireless *Maintenance Guide*.

Verify Synchronization

To verify that all elements have been synchronized correctly, navigate to the VNS tab on both the primary and secondary controllers, and confirm that the topologies, WLAN services, roles and desired VNSs are displayed as **[synchronized]**.

You can verify this by selecting the appropriate tabs and then inspecting the Synchronized flags or by navigating to **VNS > Global > Sync Summary**.

Configuration synchronization:

- VNS configuration related synchronization will be supported with legacy or fast failover availability configuration as long as there is an availability link established.
- Synchronization for VNS, WLAN Services, Roles, Topologies, and Rate Limit Profiles can be enabled/disabled individually.
- VNS, WLAN Service, Role, Topology, and Rate Limit Profile configuration will be dynamically synchronized when synchronization is enabled individually between a pair of controllers.

MU session synchronization:

- MU session synchronization will be supported only when there is fast failover configured between two controllers.
- If mobility is disabled, MU session with Bridge Traffic Locally at AP, Bridge Traffic Locally at Controller, and Routed topologies will all be synchronized between a pair of controllers.
- If mobility is enabled, an MU session with Routed topologies will not be synchronized.

Viewing SLP Activity

In normal operations, the primary controller registers as an SLP service called ac_manager. The controller service directs the APs to the appropriate controller. During an outage, if the remaining controller is the secondary controller, it registers as the SLP service ru_manager.

To view SLP activity:

- 1 From the top menu, click **AP**.
- 2 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:

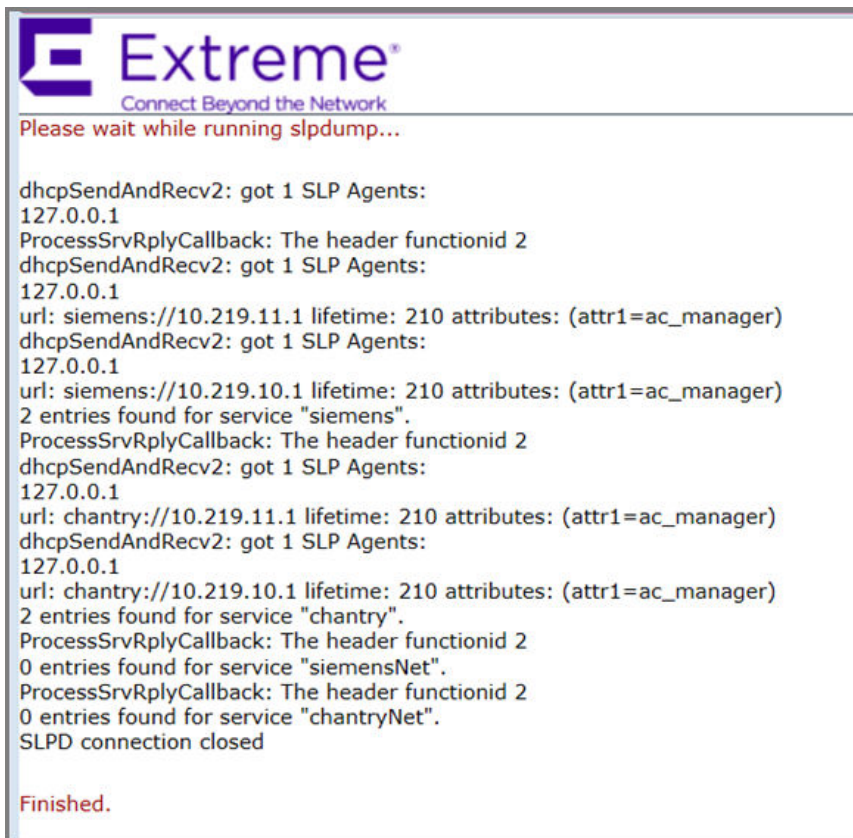
Confirm password:

Secure Cluster:

Cluster Shared Secret:

Use Cluster Encryption

- To confirm SLP registration, click **View SLP Registration**. A screen displays the results of the diagnostic sldump tool, to confirm SLP registration.



The screenshot shows a terminal window with the Extreme logo and tagline 'Connect Beyond the Network'. The text inside the terminal reads: 'Please wait while running sldump...'. The output shows the results of the sldump tool, including DHCP send and receive messages, SLP agent discovery for 'siemens' and 'chantry' services, and the final status 'Finished.'.

```
Extreme®  
Connect Beyond the Network  
Please wait while running sldump...  
  
dhcpSendAndRecv2: got 1 SLP Agents:  
127.0.0.1  
ProcessSrvRplyCallback: The header functionid 2  
dhcpSendAndRecv2: got 1 SLP Agents:  
127.0.0.1  
url: siemens://10.219.11.1 lifetime: 210 attributes: (attr1=ac_manager)  
dhcpSendAndRecv2: got 1 SLP Agents:  
127.0.0.1  
url: siemens://10.219.10.1 lifetime: 210 attributes: (attr1=ac_manager)  
2 entries found for service "siemens".  
ProcessSrvRplyCallback: The header functionid 2  
dhcpSendAndRecv2: got 1 SLP Agents:  
127.0.0.1  
url: chantry://10.219.11.1 lifetime: 210 attributes: (attr1=ac_manager)  
dhcpSendAndRecv2: got 1 SLP Agents:  
127.0.0.1  
url: chantry://10.219.10.1 lifetime: 210 attributes: (attr1=ac_manager)  
2 entries found for service "chantry".  
ProcessSrvRplyCallback: The header functionid 2  
0 entries found for service "siemensNet".  
ProcessSrvRplyCallback: The header functionid 2  
0 entries found for service "chantryNet".  
SLPD connection closed  
  
Finished.
```


14 Configuring Mobility

Mobility Overview
Mobility Domain Topologies
Configuring a Mobility Domain

Mobility Overview

The ExtremeWireless system allows up to 12 controllers on a network to discover each other and exchange information about a client session. This technique enables a wireless device user to roam seamlessly between different APs on different controllers.

The solution introduces the concept of a mobility manager; one controller on the network is designated as the mobility manager and all others are designated as mobility agents.

The wireless device keeps the IP address, and the service assignments it received from its home controller—the controller that it first connected to. The WLAN Service on each controller must have the same SSID and RF privacy parameter settings.

You have two options for choosing the mobility manager:

- Rely on SLP with Option 78
- Define at the agent the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended to provide tighter control of the registration steps for multi-domain installations.

The controller designated as the mobility manager:

- Is explicitly identified as the manager for a specific mobility domain. Agents connect to this manager to establish a mobility domain.
- Defines, at the agent, the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Uses SLP, if this method is preferred, to register itself with the SLP Directory Agent as Extreme NetworksNet.
- Defines the registration behavior for a multi-controller mobility domain set:
 - **Open mode** — A new agent is automatically able to register itself with the mobility manager and immediately becomes part of the mobility domain.
 - **Secure mode** — The mobility manager does not allow a new agent to automatically register. Instead, the connection with the new agent is placed in a pending state until the administrator approves the new device.
- Listens for connection attempts from mobility agents.
- Establishes connections and sends a message to the mobility agent specifying the heartbeat interval, and the mobility manager's IP address if it receives a connection attempt from the agent.

- Sends regular heartbeat messages containing wireless device session changes and agent changes to the mobility agents and waits for a returned update message.
- Establishes a connection to an optional backup mobility manager that can be configured to back up the primary mobility manager.

The controller designated as a mobility agent does the following:

- Uses SLP or a statically configured IP address to locate the mobility manager.
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Attempts to establish a TCP/IP connection with the mobility manager.
- Connects to an optional backup mobility manager that can be configured to back up the primary mobility manager.
- Sends updates, in response to the heartbeat message, on the wireless device users and the data tunnels to the mobility manager.

If a controller configured as the mobility manager is lost, with a backup mobility manager configured, the following occurs:

- If enabled, the controller establishes a connection to the optional backup mobility manager. When a failure occurs, the backup manager becomes the primary manager and control tunnels are re-negotiated. The data tunnels are not affected. When the primary manager comes back online, the backup manager detects the higher priority manager and switches back to agent (passive) mode.

If a controller configured as the mobility manager is lost, without a backup mobility manager, the following occurs:

- Agent to agent connections remain active.
- The mobility agents continue to operate based on the mobility information last coordinated before the manager link was lost. The mobility location list remains relatively unaffected by the controller failure. Only entries associated with the failed controller are cleared from the registration list, and users that have roamed from the manager controller to other agents are terminated and required to re-register as local users with the agent where they are currently located.
- The data link between active controllers remains active after the loss of a mobility manager.
- Mobility agents continue to use the last set of mobility location lists to service known users.
- Existing users remain in the mobility scenario, and if the users are known to the mobility domain, they continue to be able to roam between connected controllers.
- New users become local at attaching controller.
- Roaming to another controller resets session.

The mobility network that includes all the wireless controllers and the APs is called the Mobility Domain.



Note

The mobility feature is not backward compatible. This means that all the controllers in the mobility domain must be running the most recent controller software release.

Mobility Domain Topologies

You can configure a mobility domain in the following scenarios:

- Mobility domain without availability
- Mobility domain with availability
- Mobility domain with session availability



Note

When configuring a mobility domain with availability or session availability, synchronize time on all the wireless controllers that are part of your mobility domain. For more information, see [Configuring Network Time](#) on page 88.

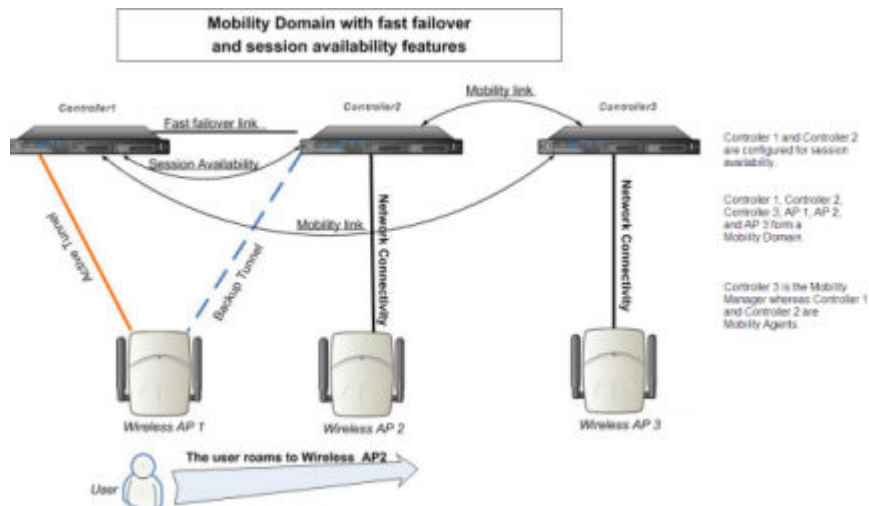


Figure 131: Mobility Domain with Fast Failover and Session Availability Features

- The user's home session is with Controller1.
- When the user roams from wireless AP 1 to wireless AP 2, he establishes his home session with Controller2.
- When the user roams, AP 1 receives a notification that the user has roamed away following which it marks the user session as "inactive". Consequently, no statistics are sent to the Controller 1 for that user.
- In response to the heart beat message from the mobility manager (Controller 3), the Controller 2 sends updates that the user has a new home on Controller 2. Upon receiving the updates, the mobility manager updates its own tables.



Note

The mobility manager's heart beat time is configurable. If you are configuring a mobility domain with session availability, you should configure the heart beat time as one second to enable the mobility manager to update its tables quickly.

- If a failover takes place, and the user is still associated with AP 1:
 - AP1 fails over, and establishes an active session with Controller 2.
 - In response to the heart beat message from the mobility manager (Controller 3), the Controller 2 sends updates to the mobility manager on the failover AP and its user.
- If a failover takes place, and the user has roamed to wireless AP 2:
 - As part of roaming, the user's home session moves from Controller 1 to Controller 2.
 - AP1 establishes active session with Controller 2. AP 2 is not impacted by the failover.

Configuring a Mobility Domain

When configuring a mobility domain with availability or session availability, synchronize time on all the wireless controllers that are part of your mobility domain. For more information, see [Configuring Network Time](#) on page 88.

Designating a Mobility Manager

To designate a mobility manager:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Services > Mobility Manager**.
- 3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options are displayed.

The screenshot shows the 'Mobility Manager Settings' page in a web interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller' (selected), 'AP', 'VNS', and 'Radar'. The left sidebar has 'Administration', 'Logs', 'Network', 'Services' (selected), 'Location-based Service', and 'Mobility Manager'. The main content area is titled 'Mobility Manager Settings' and contains the following options:

- Mobility**
- This Wireless Controller is a Mobility Manager**
 - Port: PHY_VLAN_110 (10.47. ...)
 - Heartbeat: 5 seconds
 - SLP Registration: Disabled
 - Permission List: Agent IP Address (State)
 - Buttons: Approve, Backup mgr, Delete, Add
 - Security Mode:
 - Allow all mobility agents to connect
 - Allow only approved mobility agents to connect
- This Wireless Controller is a Mobility Agent**

- 4 Select the **This Wireless Controller is a Mobility Manager** option. The mobility manager options are displayed.
- 5 In the **Port** drop-down list, select the interface on the controller to be used for the mobility manager process. Ensure that the selected interface's IP address is routable on the network.

- 6 In the **Heartbeat** box, type the time interval (in seconds) at which the mobility manager sends a Heartbeat message to a mobility agent.

**Note**

When the mobility domain is configured for fast failover and session availability, configure the mobility manager's heart beat time as one second.

- 7 In the **SLP Registration** drop-down list, select whether to enable or disable SLP registration.
- 8 In the **Permission** list, select the agent IP addresses you want to approve that are in pending state, by selecting the agent and clicking **Approve**. New agents are only added to the domain if they are approved.
 - To add a controller to the mobility domain, type the agent IP address in the box, and then click **Add**. This can only be done from the primary manager.
 - To assign a backup manager, select a controller from the Permission List, and click **Backup mgr**.
 - To delete a controller, click the controller in the list, and then click **Delete**. This can only be done from the primary manager.
- 9 Select the **Security Mode** option:
 - **Allow all mobility agents to connect** — All mobility agents can connect to the mobility manager.
 - **Allow only approved mobility agents to connect** — Only approved mobility agents can connect to the mobility manager.
- 10 Click **Save**.

**Note**

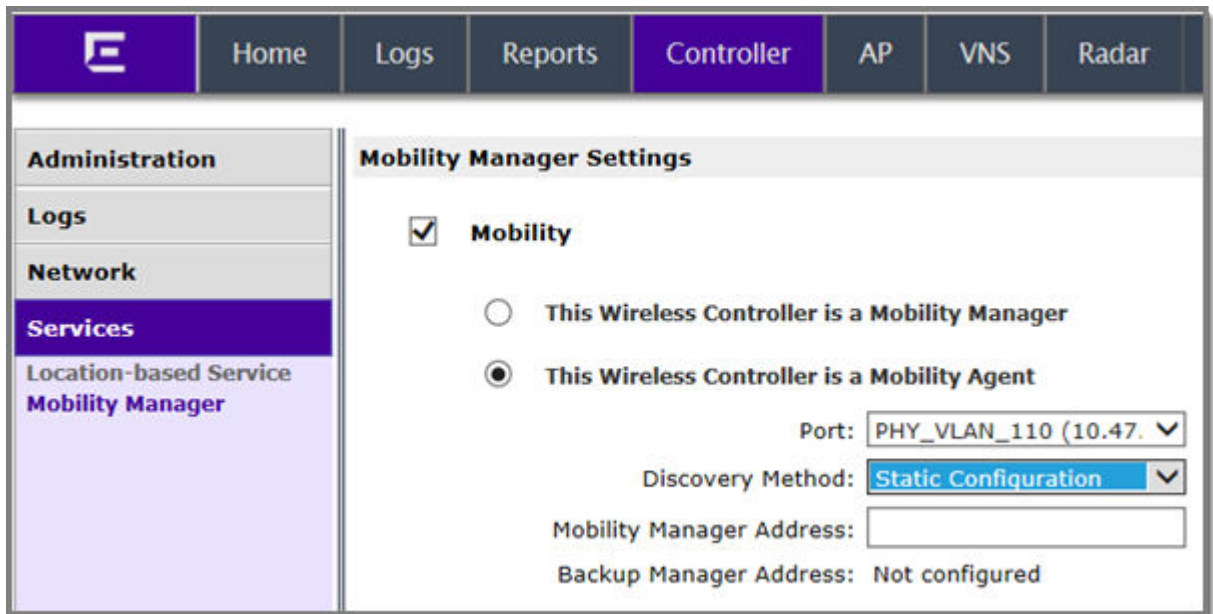
If you set up one wireless controller on the network as a mobility manager, all other controllers must be set up as mobility agents.

Designating a Mobility Agent

To designate a mobility agent:

- 1 From the top menu, click **Controller**.
- 2 In the left pane, click **Services > Mobility Manager**.
- 3 Select the **Mobility** checkbox. The controller mobility options are displayed.

- 4 Select the **This Wireless Controller is a Mobility Agent** option. The mobility agent options are displayed.



The screenshot shows the 'Mobility Manager Settings' configuration page. The left sidebar has a menu with 'Administration', 'Logs', 'Network', 'Services', 'Location-based Service', and 'Mobility Manager'. The 'Services' menu is expanded, and 'Mobility Manager' is selected. The main content area is titled 'Mobility Manager Settings' and contains the following options:

- Mobility**
 - This Wireless Controller is a Mobility Manager
 - This Wireless Controller is a Mobility Agent
- Port: PHY_VLAN_110 (10.47) (dropdown menu)
- Discovery Method: Static Configuration (dropdown menu)
- Mobility Manager Address: (text input field)
- Backup Manager Address: Not configured

- 5 From the **Port** drop-down list, select the **port** on the controller to be used for the mobility agent process. Ensure that the port selected is routable on the network.
- 6 From the **Discovery Method** drop-down list, select one of the following:
- **SLPD** — Service Location Protocol Daemon, a background process acting as an SLP server, provides the functionality of the Directory Agent and Service Agent for SLP. Use SLP to locate the area mobility manager controller.
 - **Static Configuration** — You must provide the IP address of the mobility manager manually. Defining a static configuration for a mobility manager IP address bypasses SLP discovery.
- 7 In the **Mobility Manager Address** box, type the IP address for the designated mobility manager. The **Backup Manager Address** box displays the IP address of the backup controller.
- 8 Click **Save**.

For information about viewing mobility manager displays, see [Viewing Mobility Reports](#) on page 596.

15 Working with Third-party APs

Defining Authentication by Captive Portal for the Third-party AP WLAN Service
Defining the Third-party APs List
Defining Policy Rules for the Third-party APs

Defining Authentication by Captive Portal for the Third-party AP WLAN Service

802.1x Authentication is not supported directly by the wireless controller. However, this type of authentication can be supported by the actual third-party AP. All other options for authentication are supported at the controller.

- 1 On the **WLAN configuration** window for the third-party WLAN Service, click the **Auth & Acct** tab.
- 2 In the **Authentication Mode** drop-down list, click **Internal** or **External**, and then click **Configure**.
- 3 Define the Captive Portal configuration as described in [Configuring Captive Portal for Internal or External Authentication](#) on page 302.

Defining the Third-party APs List

- 1 In the **WLAN Services** panel, select the third-party WLAN Service.
- 2 In the **IP Address** field, type the IP address of a third-party AP.
- 3 In the **Wired MAC Address** field, type the MAC address of the AP.
- 4 Click **Add** to add the AP to the list.
- 5 Repeat for all third-party APs to be assigned to this WLAN Service.

Defining Policy Rules for the Third-party APs

- 1 Because the third-party APs are mapped to a physical topology, you must define the Exception filters on the physical topology, using the **Exception Filters** tab. For more information, see [Exception Filtering](#) on page 234.
- 2 Define policy rules that allow access to other services and protocols on the network such as HTTP, FTP, and SNMP.
- 3 On the **Multicast Filters** tab, select **Enable Multicast Support** and configure the multicast groups whose traffic is allowed to be forwarded to and from the VNS using this topology. For more information, see [Multicast Filtering](#) on page 237.

In addition, modify the following functions on the third-party AP:

- Disable the AP's server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the controller with VNS information.
- Disable the third-party AP's layer-3 IP routing capability and set the access point to work as a layer-2 bridge.

The following are the differences between third-party APs and APs on the Extreme Networks ExtremeWireless system:

- A third-party AP exchanges data with the controller's data port using standard IP over Ethernet protocol. The third-party access points do not support the tunnelling protocol for encapsulation.
- For third-party APs, the VNS is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A controller cannot directly control or manage the configuration of a third-party access point.
- Third-party APs are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other VNS.
- Roaming from third-party APs to wireless APs and vice versa is not supported.

16 Working with ExtremeWireless Radar

Radar Overview
Radar Components
Radar License Requirements
Radar Scan Profiles
Enabling the Analysis Engine
Viewing Existing Scan Profiles
Adding a New Scan Profile
Configuring an In-Service Scan Profile
Configuring a Guardian Scan Profile
Maintaining the Radar List of APs
Working with Radar Reports

Radar Overview

Radar is a set of advanced, intelligent features for managing the wireless environment. Radar includes advanced features for:

- Device location tracking
- Wireless-Intrusion-Detection and Wireless-Intrusion-Prevention (WIDS-WIPS)
- Advanced load balancing capability

Radar provides a basic solution for discovering unauthorized devices within the wireless coverage area. Radar performs basic RF network analysis to identify unmanaged APs and personal ad-hoc networks. The Radar feature set includes: intrusion detection, prevention and interference detection.

All APs can provide WIDS and traffic forwarding functionality, simultaneously and, if configured to do so, will apply countermeasures to detected wireless intrusions.

All APs (except 3705) can be placed in Guardian mode. In this mode, the AP dedicates both radios for intrusion detection and prevention functions. Guardians are capable of detecting and mitigating attacks on wireless channels that are not being used for traffic forwarding by the authorized network.

When controllers are configured in an availability pair, the Radar feature operates in High Availability mode, allowing Radar to retain its configuration, historical, and runtime data in the case of an availability pair controller failure. In High Availability mode, the configuration and runtime on both controllers is synchronized.

Radar Components

Figure 132 illustrates the major components of Radar.

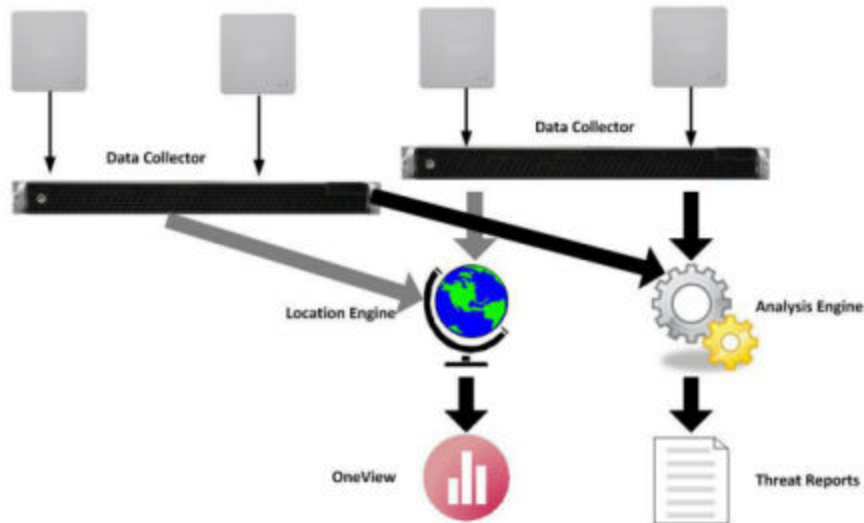


Figure 132: Radar System Components

Analysis Engine Overview

Radar requires that one controller host the Analysis Engine, and a data collector application, is installed on each controller. The data collector receives and manages the RF scan messages sent by each AP. The data collector forwards to the Analysis Engine lists of all connected wireless APs, third-party APs and RF scan information collected from participating APs.

The Analysis Engine processes the scan data from the data collectors through algorithms that make decisions about whether any of the detected APs or clients are threats or are running in an unsecure environment (for example, in ad-hoc mode).

APs must be part of a Radar scan profile to participate in WIDS-WIPS activity. A scan profile is a collection of WIDS-WIPS configuration options that can be assigned to appropriate APs. The actual configuration options depend on whether the profile is an In-Service or Guardian scan profile.

The Analysis Engine relies on a database of connected devices on the Extreme Networks ExtremeWireless system. The database is basically a compiled list of all APs and clients connected to the controller. The Analysis Engine compares the data from the data collector with the database of known devices. For more information on enabling the Analysis Engine, see [Enabling the Analysis Engine](#) on page 520.

Radar Functionality on the Controller

The Analysis Engine can run on a standalone controller or on a High Availability pair. The controller's Analysis Engine works only with local data collectors and with data collectors of the controller's availability partner.

Radar Functionality on the Wireless AP

An AP can be assigned to only one scan profile and only needs to be added to a profile if it is to be used for scanning.

APs run a radio frequency (RF) scanning task.

The APs scan for threats and perform countermeasures while simultaneously providing full traffic forwarding services including the application of role.



Note

When you enable countermeasures, the countermeasures apply to threats on channels that receive forwarded traffic.

All APs, except 3705, support Guardian mode profile. In Guardian mode, the APs rapidly sweep across multiple channels. This allows for threat detection on channels that are being used by APs that are not authorized to provide service. However, the more channels the AP has to defend concurrently, the less thoroughly it can defend any one channel. The AP will only defend a channel if an actual threat is detected on that channel, and if the Analysis Engine on the controller is able to distribute responsibility for dealing with concurrent active threats among multiple APs.



Note

If an AP is part of a WDS/Mesh link, you cannot configure it to act as a Guardian AP in Radar.

Radar License Requirements

Radar functionality is controlled by capacity licenses installed on the controller and activated as an option key. For more information on the Option Key, see [Applying Product License Keys](#) on page 48. Any AP assigned to an In-Service scan profile counts as 1 against the licensed Radar capacity. The base capacity for all controllers is 2, and any capacity increment can be installed on any controller.

AP Limitations

The maximum number of APs that can be licensed for Radar is twice the platform limit for local APs. Once the maximum number of APs is reached, no new licenses can be installed.

Radar Scan Profiles

Radar scan profiles provide the ability to organize scans for rogue activity based on a specific set of parameters such as radio assignments and desired channels. APs can be selected from a list of Assigned APs or a new AP can be added to the scan profile. An AP can only belong to one scan profile.

Radar provides In-Service and Guardian scan profiles.

- Any AP can use the In-Service scan profile. For more information, see [Configuring an In-Service Scan Profile](#) on page 523.
- All APs, except 3705, can use the Guardian scan profile. For more information, see [Configuring a Guardian Scan Profile](#) on page 528.

In-Service Scan Profiles

In-Service scan profiles work with any AP type and include the following:

- A set of countermeasure that lists possible prevention options to counter specific types of threats. For more information, see [In-Service Scan Profile Prevention Settings](#) on page 524.
- Support for automatic blacklisting, which automatically removes network access from devices performing certain types of wireless attacks. For more information, see [Blacklisted Clients](#) on page 546. The administrator can configure the length of time that a device remains on the blacklist.

Guardian Scan Profiles

Guardian scan profiles work with all AP types (except AP3705) and include the following:

- An AP operating in Guardian mode does not bridge traffic and instead devotes all of the AP's resources to threat detection and countermeasures.
- An AP is added to a Guardian scan mode in its entirety. There is no option to dedicate one radio to scanning and the other to forwarding.
- An AP assigned to a Guardian scan profile stops providing any services (WLAN service, load groups, site) immediately.
- A list of all possible channels that the Guardian AP could scan. Each channel has a checkbox which when checked enables scanning by any AP in the group.
- A set of countermeasure that lists possible prevention options to counter specific types of threats. For more information, see [In-Service Scan Profile Prevention Settings](#) on page 524.
- Support for automatic blacklisting which allows the administrator to list which MAC addresses should be allowed or denied on the network. For more information, see [Blacklisted Clients](#) on page 546.
- Addresses added to the blacklist manually are there until they are manually removed. If blacklisting clients is enabled, you can set the maximum amount of time a device can be blacklisted.

Enabling the Analysis Engine

Before using Radar, you must enable and define the Analysis and Data Collector Engines.

If using In-Service scan profiles, only the controller itself and its availability pair report to the Analysis Engine. For more information, see [Configuring an In-Service Scan Profile](#) on page 523.

To enable the Analysis Engine:

- 1 From the top menu, click **Radar**.
The **Configuration > Engine Settings** screen displays.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

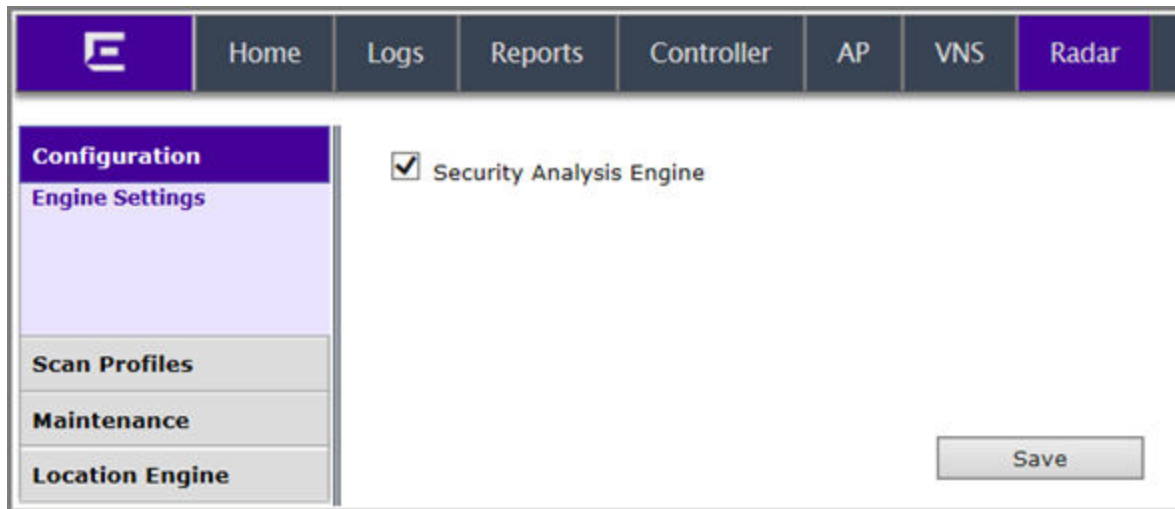


Figure 133: Radar Engine Settings

Viewing Existing Scan Profiles

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Scan Profiles**.

The **Scan Profiles** screen displays.

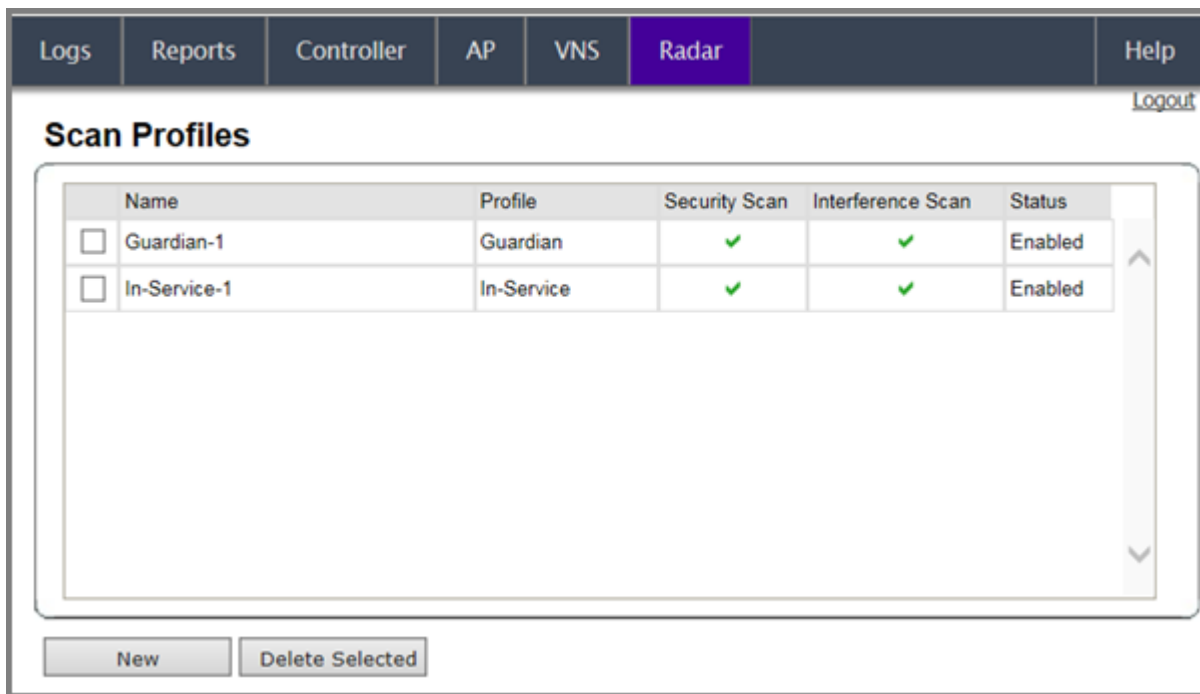






Figure 134: In-Service Scan Profiles

Table 98: Scan Profiles - Fields and Buttons

Field/Button	Description
Name	The name of the scan profile.
Profile	In-Service or Guardian.
Security Scan	<p>Indicates whether the profile enables security scanning on APs assigned to the profile.</p> <p></p> <p>Indicates that the scan profile enables security scanning.</p> <p></p> <p>Indicates that the scan profile does not enable security scanning.</p>
Interference Scan	<p>Interference classification compares patterns in RF interference to known interference patterns to help identify the source of the interference.</p> <p></p> <p>Indicates that the interference scan classification is enabled on specific APs assigned to the profile.</p> <p></p> <p>Indicates that the interference scan classification is not enabled on specific APs assigned to the profile.</p>
Status	<p>Enabled: Indicates that the scan profile is enabled (for example, whether the APs assigned to the profile are scanning in accordance with the profile). Scan profiles are Enabled if either security scanning or interference scanning is enabled.</p> <hr/> <p>Disabled: Indicates that the scan profile is disabled. A disabled profile means the profile is defined but any APs assigned to the profile are not performing scans.</p>
New	Click to create a new scan profile (see Adding a New Scan Profile on page 522).
Delete Selected	Click to delete the selected scan profile.

Adding a New Scan Profile

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 Select **Scan Profiles**.
- 4 From the **Scan Profiles** screen, click **New**.

- 5 In the **Add Scan Profile** dialog, select the profile type:
 - Guardian
 - In-Service

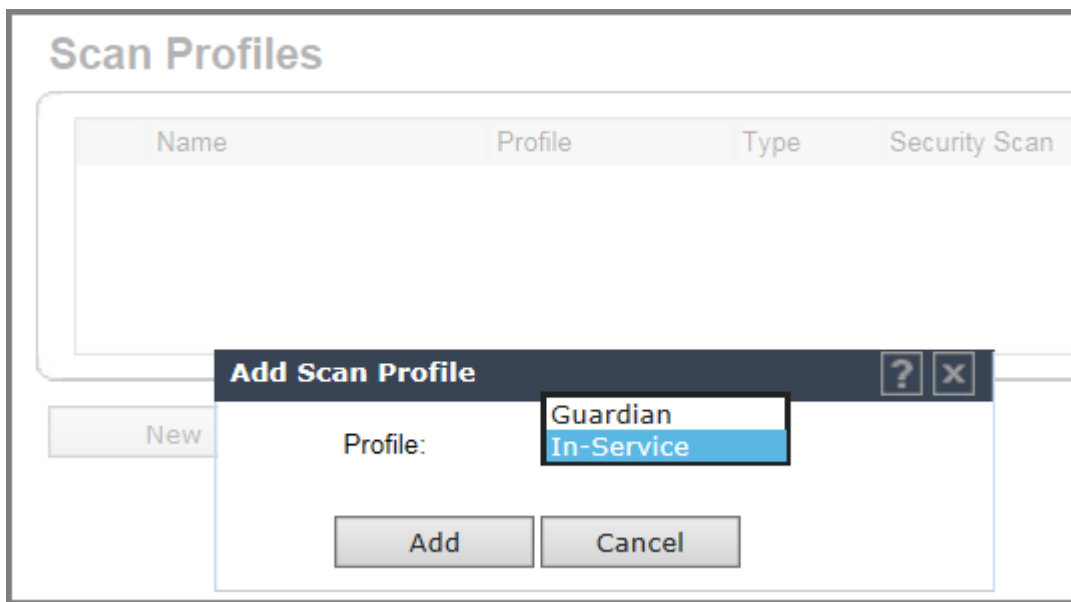


Figure 135: Add Scan Profile

- 6 For information about configuring the profile:
 - [Configuring a Guardian Scan Profile](#) on page 528.
 - [Configuring an In-Service Scan Profile](#) on page 523.

Configuring an In-Service Scan Profile

Configure the following for an In-Service scan profile:

- Detection Settings
- Prevention Settings
- List of Assigned APs

In-Service Scan Profile Detection Settings



Note

Once an In-Service scan profile is created, the **Detection** tab appears.

Select the **Detection** tab.

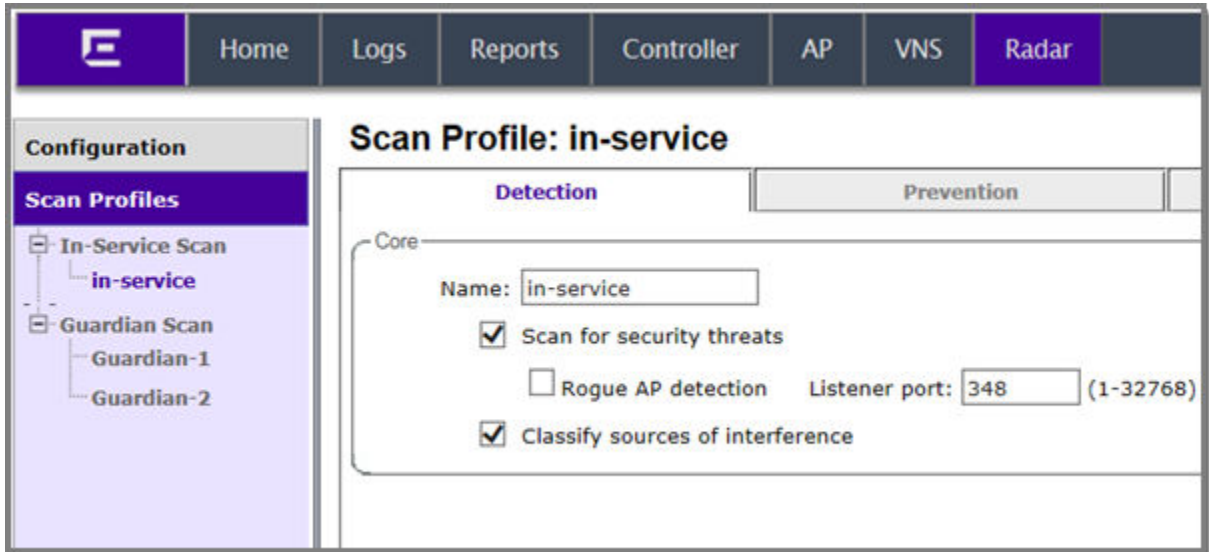


Figure 136: Detection Settings

From the Core pane, type a unique name for the scan profile and configure the following detection options:

- Scan for security threats. For more information, see [Security Threats](#) on page 543.
- Rogue AP detection. Select this option to detect rogue APs serving open SSIDs (for example an AP attached to an Ethernet wall jack and the AP is running an open SSID). If a rogue AP is detected, countermeasures can be optionally applied to prevent any station from using this rogue AP.
- Listener port: Enter the UDP port for rogue AP detection.
- Classify sources of interference. Interference classification compares patterns in RF interference to known interference patterns to help identify the source of the interference. All APs based on the AP371x, AP38xx, and AP39xx architecture are capable of performing interference classification.
- Click **Save**.

In-Service Scan Profile Prevention Settings

Radar provides multiple countermeasures which can be enabled in an In-Service scan profile. The level of prevention for the profile is dependent on the countermeasures selected. For more information on the Radar threat categories for which countermeasures can be applied, see [Radar Scan Profiles](#) on page 519.

When Radar WIDS-WIPS is enabled, all detected threats are reported when they start and when they stop. The reports are available in the controller's event logs and can be streamed off the controller using SNMP and syslog. These event reports are always generated regardless of which other countermeasures are enabled. For more information on these reports, see [Working with Radar Reports](#) on page 542.

Selecting Countermeasures

Countermeasures mitigate the impact of a security threat:

- Sending standard 802.11 deauthentication frames to prevent stations from associating to threat devices.

- Rate limiting flooded frames. This can prevent floods from propagating through the AP to the wired network.
- Blacklisting attacking devices to prevent them from gaining access to the network.

Countermeasures are enabled on a per-scan-profile basis. Some scan profiles can have countermeasures enabled while others cannot.

To select a specific countermeasure:

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Scan Profiles**.
- 3 Select an In-Service scan profile and click the **Prevention** tab.

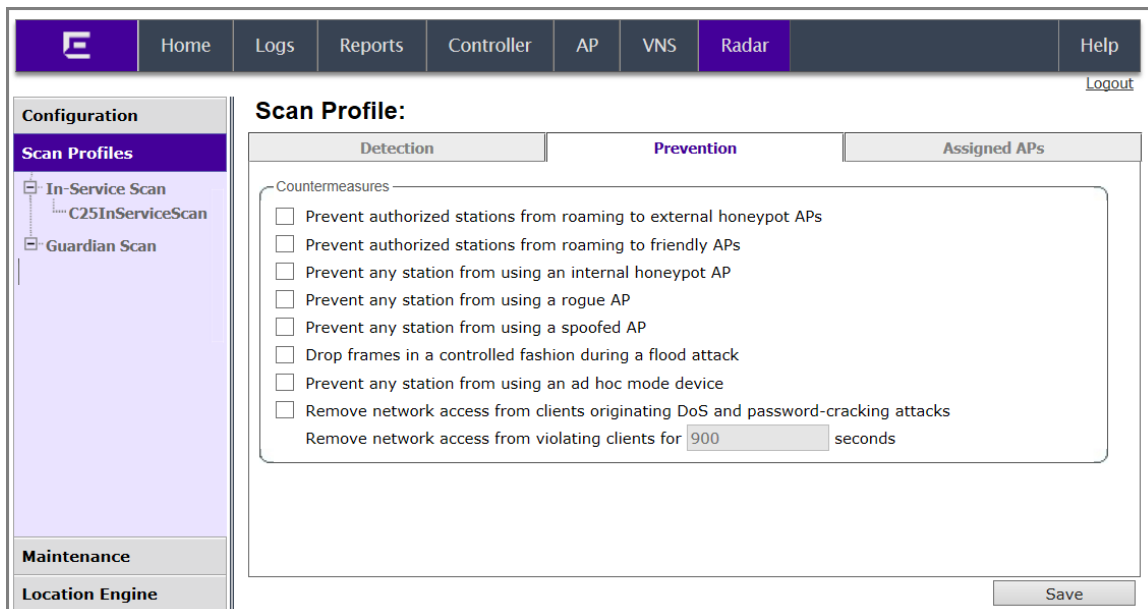


Figure 137: Prevention Settings

Table 99: Prevention Tab - Fields and Buttons

Field/Button	Description
Countermeasures	
Prevent authorized stations from roaming to external honeypot APs	An external honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport
Prevent authorized stations from roaming to friendly APs	Friendly APs are APs that are not part of the authorized network, but they operate in the vicinity of the authorized network.
Prevent any station from using an internal honeypot AP	An internal honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized network.
Prevent any station from using a rogue AP	A rogue AP is an unauthorized AP connected to the authorized wired network.

Table 99: Prevention Tab - Fields and Buttons (continued)

Field/Button	Description
Prevent any station from using a spoofed AP	A spoofed AP is an AP that is not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.
Drop frames in a controlled fashion during a flood attack	Prevents some types of Denial of Service (DoS) attack from affecting the authorized network instead of just the target AP. For example, rate limiting the flooded frames.
Prevent any station from using an ad hoc mode device	Deauthentication messages are used to prevent devices from using an ad hoc mode device.
Remove network access from clients originating DoS and password-cracking attacks	Prevents propagation of the DoS attack from the AP to the authorized network. Many types of DoS attack involve deluging an AP with a large volume of messages of one or two specific types. When this option is enabled, the AP will apply rate limits to the specific type of frame that is being deluged. The selected clients for this countermeasure are denied access to the network for the amount of time that is specified in " Remove network access from violating clients for a period of time."
Remove network access from violating clients for a period of time	Enter a numeric value in seconds.
New	Click to create a new scan profile. For more information, see Adding a New Scan Profile on page 522.
Delete	Click to delete the selected scan profile.
Save	Click to save changes.

Viewing the List of Assigned APs

The list of Assigned APs is all the APs reported by the data collectors, and it automatically appear once a scan profile is created. To view the list of APs assigned to this In-Service scan profile, click the **Assigned APs** tab.

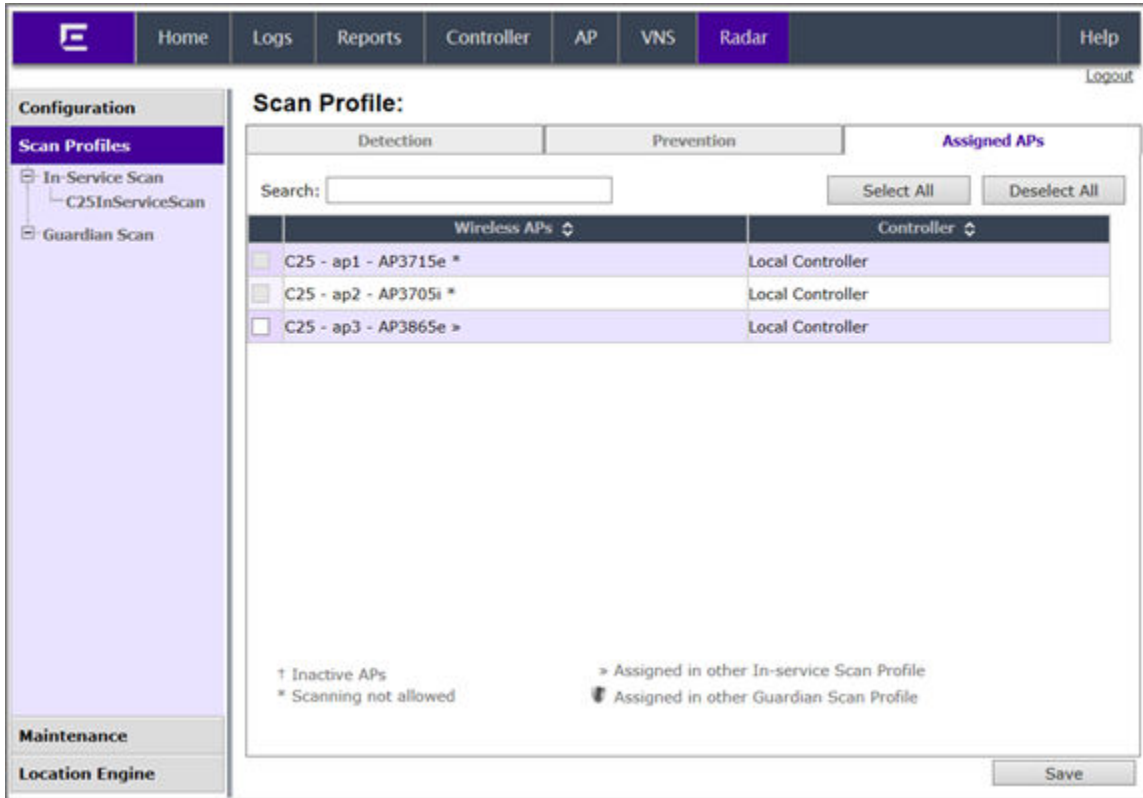


Figure 138: Assigned APs

Table 100: Assigned APs Tab - Fields and Buttons

Field/Button	Description
Wireless APs	Identifies the wireless APs assigned to this In-Service Scan profile. May include the AP name or serial number.
Controller	Identifies the controller associated with the wireless AP. An IP address indicates a remote data collector. Local Controller indicates a controller local to the AP.
Search	To search for an AP in the list, enter the name of the AP and press Enter .
Select All	Select all APs in the list.
Deselect All	Clear the selection of all APs in the list.
Save	Click to save changes.

The list of Assigned APs are APs that are available to any scan profile. However, an AP can only be assigned to one scan profile.

Related Links

[Assigning an AP to an In-Service Scan Profile](#) on page 527

Assigning an AP to an In-Service Scan Profile

To assign an AP to an In-Service scan profile:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Scan Profiles**.
- 4 Select an In-Service scan profile, and click the **Assigned APs** tab.
- 5 Select an AP from the list of Assigned APs and click **Save**.

Configuring a Guardian Scan Profile

Configure the following for a Guardian scan profile:

- Detection Settings
- Prevention Settings
- List of Assigned APs

Guardian Scan Profile Detection Settings



Note

Once a new Guardian Scan Profile is created, the Detection tab appears.

Figure 139: Detection Settings

- 1 In the **Name** box, type a unique name for this scan profile.

Select from the following detection options:

- Scan for security threats. For more information, see [Security Threats](#) on page 543.
 - Classify sources of interference. Interference classification compares patterns in RF interference to known interference patterns to help identify the source of the interference. All APs based on the AP371x, AP38xx, and AP39xx architecture are capable of performing interference classification.
- 2 Under Channels to Monitor:
 - Click the **2.4 GHz** tab and select channels to be monitored within this band for the scan profile.
 - Click the **5 GHz** tab and select channels to be monitored within this band for the scan profile.

Guardian Scan Profile Prevention Settings

Radar provides multiple countermeasures which can be enabled in a Guardian scan profile. The level of prevention for the profile is dependent on the countermeasures selected. For more information on the Radar threat categories for which countermeasures can be applied, see [Radar Scan Profiles](#) on page 519.

When Radar WIDS-WIPS is enabled, all detected threats are reported when they start and when they stop. The reports are available in the controller's event logs and can be streamed off the controller using SNMP and syslog. These event reports are always generated regardless of which other countermeasures are enabled. For more information on these reports, see [Working with Radar Reports](#) on page 542.

Selecting Countermeasures

Countermeasures mitigate the impact of a security threat. Three main countermeasures are used by the Guardian APs:

- Sending standard 802.11 deauthentication frames to prevent stations from associating to threat devices.
- Rate limiting flooded frames. This can prevent floods from propagating through the AP to the wired network.
- Blacklisting attacking devices to prevent them from gaining access to the network.

To select a specific countermeasure:

Countermeasures are enabled on a per-scan-profile basis. Some scan profiles can have countermeasures enabled while others cannot.

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Scan Profiles**.

- 4 Select a Guardian scan profile and click the **Prevention** tab.

Scan Profile:

Detection **Prevention** Assigned APs

Countermeasures

- Prevent authorized stations from roaming to external honeypot APs
- Prevent authorized stations from roaming to friendly APs
- Prevent any station from using an internal honeypot AP
- Prevent any station from using a rogue AP
- Prevent any station from using a spoofed AP
- Drop frames in a controlled fashion during a flood attack
- Prevent any station from using an ad hoc mode device
- Remove network access from clients originating DoS and password-cracking attacks

Remove network access from violating clients for seconds

Defense Options

Maximum number of channels per radio to defend concurrently

1 2 3 4

Figure 140: Prevention Settings

- 5 Select desired prevention method.
- 6 Select number of channels per radio to defend concurrently. Number of defended channels can be between 1 and 4.

Table 101: Prevention Tab - Fields and Buttons

Field/Button	Description
Countermeasures	
Prevent authorized stations from roaming to external honeypot APs	An external honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport
Prevent authorized stations from roaming to friendly APs	Friendly APs are APs that are not part of the authorized network, but they operate in the vicinity of the authorized network.
Prevent any station from using an internal honeypot AP	An internal honeypot is an AP that is attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized network.
Prevent any station from using a rogue AP	A rogue AP is an unauthorized AP connected to the authorized wired or wireless network.
Prevent any station from using a spoofed AP	A spoofed AP is an AP that is not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.

Table 101: Prevention Tab - Fields and Buttons (continued)

Field/Button	Description
Drop frames in a controlled fashion during a flood attack	Prevents some types of Denial of Service (DoS) attack from affecting the authorized network instead of just the target AP. For example, rate limiting the flooded frames.
Prevent any station from using an ad hoc mode device	Deauthentication messages are used to prevent devices from using an ad hoc mode device.
Remove network access from clients originating DoS and password-cracking attacks	Prevents propagation of the DoS attack from the AP to the authorized network. Many types of DoS attack involve deluging an AP with a large volume of messages of one or two specific types. When this option is enabled, the AP will apply rate limits to the specific type of frame that is being deluged. The selected clients for this countermeasure are denied access to the network for the amount of time that is specified in "Remove network access from violating clients for a period of time."
Remove network access from violating clients for a period of time	Enter a numeric value in seconds.
Defense Options	
Maximum number of channels per radio to defend concurrently	Click the slider to select the number of channels desired.
New	Click to create a new Guardian scan profile. For more information, click Adding a New Scan Profile on page 522.
Delete	Click to delete the selected Guardian scan profile.
Save	Click to save changes.

Viewing the List of Assigned APs

The list of Assigned APs is a list of all APs reported by the data collectors. Assigned APs automatically appear once a scan profile is created. To view the list of APs assigned to this Guardian scan profile, click the **Assigned APs** tab.

Scan Profile: g11

Detection | Prevention | Assigned APs

Search:

Wireless APs	Controller	Assigned to Site/Load group/WLAN service
<input type="checkbox"/> 3715e †	Local Controller	N/N/Y
<input type="checkbox"/> 3825i » †	Local Controller	N/N/N
<input type="checkbox"/> 3865e » †	Local Controller	N/N/Y
<input type="checkbox"/> 3935i » †	Local Controller	N/N/Y
<input type="checkbox"/> name-13310619085D0000	Local Controller	N/N/N

† Inactive APs
 * Scanning not allowed
 » Assigned in other In-service Scan Profile
 ⚡ Assigned in other Guardian Scan Profile

Figure 141: Assigned APs

Table 102: Assigned APs Tab - Fields and Buttons

Field/Button	Description
Wireless APs	Identifies the wireless APs assigned to this In-Service Scan profile. May include the AP name or serial number.
Controller	Identifies the controller associated with the wireless AP. An IP address indicates a remote data collector. Local Controller indicates a controller local to the AP.
Assigned to Site/Load group/WLAN service	Indicates with a Y (Yes) or N (No) if the AP is assigned to a Site, Load Group, or WLAN Service.
Search	To search for a profile in the list, enter the full name of a scan profile and press Enter.
Select All	Select all APs in the list.
Deselect All	Clear the selection of all APs in the list.
Save	Click to save changes.

The list of Assigned APs are APs that are available to any scan profile. However, an AP can only be assigned to one scan profile.

Related Links

[Assigning an AP to a Guardian Scan Profile](#) on page 533

Assigning an AP to a Guardian Scan Profile

To assign an AP to a Guardian scan profile:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Scan Profiles**.
- 4 Select a Guardian scan profile, and click the **Assigned APs** tab.
- 5 Select an AP from the list of Assigned APs and click **Save**.



Note

All APs, except the 3705, use the Guardian scan profile.

Maintaining the Radar List of APs

Radar provides a list of APs organized in categories based on the scan results of the Analysis Engine. Radar will try to assign each discovered AP to one of these categories. If it can't find a specific category for the AP, it will assign it to the Uncategorized APs category. Uncategorized APs require manual classification. To get the best protection from Radar, classify uncategorized APs as soon as possible.

You can manually assign APs from one category to another using Radar. For more information, see [Reclassifying APs](#) on page 541.

AP Categories

APs belong to one of the following categories when they are added to the Analysis Engine database:

- **Scanning APs** - This is the subset of authorized APs configured to provide WIDS-WIPS services.
- **Friendly APs** - These are APs that are not part of the authorized network, but they operate in the vicinity of the authorized network. Friendly APs are operated by a neighboring enterprise for their own use. Authorized APs can prevent authorized devices from using friendly APs.
- **Uncategorized APs** - APs discovered by scanning APs and which do not fall into any other category. Uncategorized APs require manual classification. To get the best protection from Radar, classify uncategorized APs as soon as possible.
- **Authorized APs** - APs that can be used by devices authorized to use the network. APs can be added to the list automatically (for example, if the APs are active on the current host or the host's availability partner) or manually.
- **Prohibited APs** - These are APs that have been manually added to the Radar database so that the Radar WIDS-WIPS system will detect them and, if so configured, protect against them. An example of manually prohibited APs might be APs that were stolen from the authorized network and now could be used to generate a security breach.

Viewing the List of Scanning APs

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

- 3 In the left pane, click **Maintenance**. The **Scanning APs** screen displays.

Wireless Controllers	Wireless APs			
	Name	Serial	Profile Name	Licensed
172.20.47.10	LAB45-3705i	1225010690410000	vs-insrv-test »	✓
	LAB45-3715i	12b2694630000000	vs-insrv-test »	✓
	LAB45-3825i	14300115085D0000	vs-gr-test 🛡️	✓

Figure 142: Scanning APs

Table 103: Scanning APs - Fields and Buttons

Field/Button	Description
Wireless Controllers	Displays the name of wireless controllers reporting to the Analysis Engine on this host. Can be the IP address of another controller or "Local Controller" which represents the controller hosting this instance of the Analysis Engine.
Wireless APs	Name - Name of the Access Point
	Serial - Serial number of the Access Point
	Profile Name - Describes the scan profile. The shield icon indicates a Guardian scan profile.
	Licensed - A check mark indicates that the AP is licensed.

Viewing the List of Friendly APs

The Friendly APs page allows you to manage the list of APs that are considered to be operating in the vicinity legitimately but to which authorized devices should not roam.

To view a list of Friendly APs:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

- 3 In the left pane, click **Maintenance > Friendly APs**.

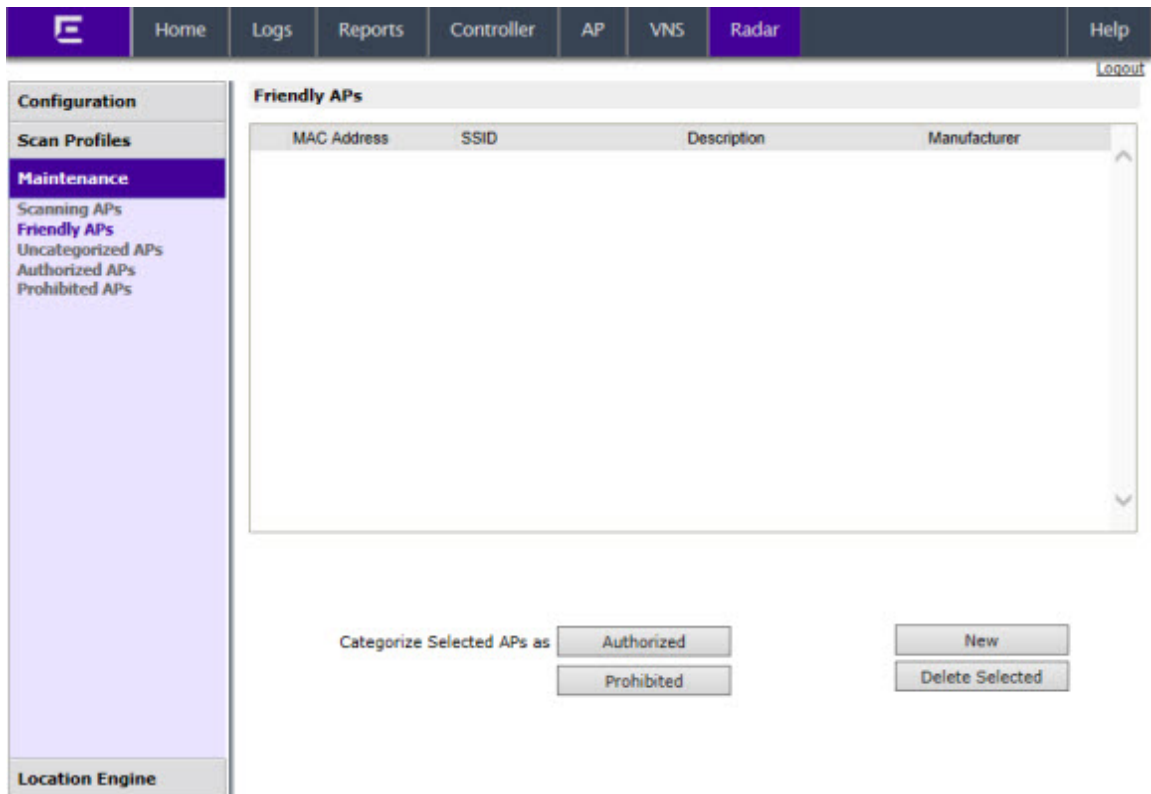


Table 104: Friendly APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address for the Friendly AP
SSID	Unique identifier attached to the header of packets sent over a wireless local-area network (WLAN) from the Friendly AP
Description	Specifies a brief description for the Friendly AP
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as Friendly APs can be reclassified as authorized or threats. For more information, see Reclassifying APs on page 541.
New	Click to create a new Friendly AP. For more information, see Adding Friendly APs on page 535.
Delete Selected	Select an AP from the list of Friendly APs, and click to delete them from the list.

Adding Friendly APs

To add a Friendly AP:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 Click **Maintenance > Friendly APs**.

- Click **New**.

The screenshot shows a dialog box titled "Friendly APs". It has a dark header bar with a question mark icon and a close button (X). The main area contains three input fields: "MAC Address:" with a text box, "SSID:" with a text box, and "Description:" with a larger text box. At the bottom, there are two buttons: "Save" and "Cancel".

Figure 143: New Friendly AP

- Configure the following parameters:
 - **MAC Address** — Specifies the MAC address of the Friendly AP
 - **SSID** — Specifies the SSID of the Friendly AP
 - **Description** — Specifies a brief description of the Friendly AP
- Click **Save**. The new access point is displayed in the Friendly APs list.

Modifying Friendly APs

To modify a Friendly AP:

- From the top menu, click **Radar**.
- If not already selected, select **Security Analysis Engine** and click **Save**.
- Click **Maintenance > Friendly APs**.
- In the **Friendly APs** list, double-click the access point you want to modify.
- Modify the access point fields as required and click **Save**.

The screenshot shows a dialog box titled "Friendly APs" with a dark header bar containing a question mark icon and a close button (X). The main area contains three input fields: "MAC Address:" with a text box containing the value "00:0F:BB:09:F0:80", "SSID:" with an empty text box, and "Description:" with an empty text box. At the bottom, there are two buttons: "Save" and "Cancel".



Note
The MAC Address field cannot be modified

Figure 144: Modify Friendly AP

Viewing the List of Uncategorized APs

Uncategorized APs are discovered but do not fall into any other category.

To view a list of Uncategorized APs:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Maintenance > Uncategorized APs**.

MAC Address	SSID	Manufacturer
<input type="checkbox"/> 00:0F:C8:00:A1:E1	suwlan	Chantry Networks
<input type="checkbox"/> 00:0F:C8:00:C8:DE	home	Chantry Networks
<input type="checkbox"/> 00:1A:EB:35:AC:B1	11d11k	Siemens Enterprise Communications GmbH & Co. KG
<input type="checkbox"/> 00:0E:8C:9B:FB:3A	cn107b-bap	Siemens AG ASD ET
<input type="checkbox"/> 00:00:00:1E:A0:09	11d11k	XEROX CORPORATION
<input type="checkbox"/> 20:83:99:43:54:5A	Prod Voice	Enterasys
<input type="checkbox"/> 00:1A:EB:14:33:38	suwlan	Siemens Enterprise Communications GmbH & Co. KG
<input type="checkbox"/> 00:0F:C8:00:AA:29	suwlan	Chantry Networks

Figure 145: Uncategorized APs

Table 105: Uncategorized APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address of the uncategorized AP
SSID	Unique identifier attached to the header of packets sent over a wireless local-area network (WLAN) from the uncategorized AP.
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as uncategorized APs can be reclassified as authorized, friendly, or prohibited. For more information, see Reclassifying APs on page 541.

Viewing the List of Authorized APs

The list of Authorized APs includes the APs that an authorized device is permitted to associate with. APs can be added to the list automatically (for example if the AP is active on the current host or its availability partner) or manually.

To view a list of Authorized APs:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.
- 3 In the left pane, click **Maintenance > Authorized APs**.

MAC Address	Description	Manufacturer
<input type="checkbox"/> 20:B3:99:43:29:18	dwrdwd	Enterasys
<input type="checkbox"/> 00:1F:45:95:42:D9	dtosedwd12	Enterasys
<input type="checkbox"/> 00:0F:BB:09:BD:C0		Nokia Siemens Networks GmbH & Co. KG
<input type="checkbox"/> 00:1A:E8:14:27:2D	tetette	Siemens Enterprise Communications GmbH & Co. KG
<input type="checkbox"/> 00:0F:BB:09:E3:DA	geege?	Nokia Siemens Networks GmbH & Co. KG

Figure 146: Authorized APs

Table 106: Authorized APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address of the authorized AP
Description	Specifies a brief description of the authorized AP
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as authorized APs can be reclassified as friendly APs. For more information, see Reclassifying APs on page 541.
New	Click to create a new authorized AP. For more information, see Adding Authorized APs on page 538.
Delete Selected	Select an AP from the list of authorized APs, and click to delete them from the list.

Adding Authorized APs

You do not have to manually add APs to the authorized AP list. The controllers create the list automatically. However, sometimes you may need to do this manually:

- An AP of a controller that is not sending information to the Analysis Engine is included on the Scanning APs screen. Devices should be able to roam between that AP and the APs of the controllers managed by the Analysis Engine.
- When adding a foreign AP (External or Internal Honeypot, or Rogue AP) to the list of Authorized APs, accidental countermeasures applied to that AP can be prevented.
- You have a third-party AP that its authorized devices should be allowed to use even though the AP is not managed by a controller.

To add an Authorized AP

- 1 To add Friendly access points manually to the **Authorized APs** list, from the Authorized APs screen, click **New**. The **Authorized APs** dialog displays.

The image shows a dialog box titled "Authorized APs". It has a dark header bar with a question mark icon and a close button (X). Below the header, there are two input fields: "MAC Address:" followed by a text box, and "Description:" followed by a longer text box. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

- 2 In the **Authorized APs** dialog, type the following:
 - **MAC Address** — Specifies the MAC address for the AP
 - **Description**— Specifies a brief description for the AP
- 3 Click **Save**. The new access point is displayed in the authorized APs list.

Viewing the List of Prohibited APs

The list of Prohibited APs are APs that you have manually added to the Radar database so that the Radar WIDS-WIPS system will detect them and, if so configured, protect against them.

To view a list of Prohibited APs:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

- 3 In the left pane, click **Maintenance > Prohibited APs**.

MAC Address	Category	Description	Manufacturer
<input type="checkbox"/> 00:1A:E8:14:27:24	External honeypot		Siemens Enterprise Communications GmbH & Co. KG
<input type="checkbox"/> 00:00:00:1E:A0:0C	Report presence only		XEROX CORPORATION
<input type="checkbox"/> 00:1A:E8:14:27:23	Internal honeypot		Siemens Enterprise Communications GmbH & Co. KG
<input type="checkbox"/> 00:1A:E8:14:27:2C	Report presence only		Siemens Enterprise Communications GmbH & Co. KG
<input type="checkbox"/> 00:0F:BB:1D:25:89	Internal honeypot	222	Nokia Siemens Networks GmbH & Co. KG
<input type="checkbox"/> 20:B3:99:43:2C:A8	Internal honeypot		Enterasys
<input type="checkbox"/> 00:1A:E8:14:27:2B	Internal honeypot	??	Siemens Enterprise Communications GmbH & Co. KG

Categorize Selected APs as

Figure 147: Prohibited APs

Table 107: Prohibited APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address of the prohibited APs
Category	Threat category
Description	Specifies a brief description of the prohibited AP
Manufacturer	Lists the AP manufacturer
Categorize Selected APs as	APs categorized as prohibited APs can be reclassified as friendly APs. For more information, see Reclassifying APs on page 541.
New	Click to create a new prohibited AP. For more information, see Adding Prohibited APs on page 540.
Delete Selected	Select APs from the list of prohibited APs, and click to delete them from the list.

Adding Prohibited APs

To add a Prohibited AP:

- 1 To add access points manually to the **Prohibited APs** list, from the **Prohibited APs** screen, click **New**. The **Prohibited APs** dialog displays.

The screenshot shows a dialog box titled "Prohibited APs". It has a title bar with a question mark icon and a close icon. The dialog contains three input fields: "MAC Address:", "Description:", and "Action:". The "Action:" dropdown menu is open, showing three options: "Report presence only" (highlighted in blue), "Treat like an internal honeypot AP", and "Treat like an external honeypot AP". At the bottom of the dialog are "Save" and "Cancel" buttons.

- 2 For **MAC Address**, specify the MAC address for the Prohibited AP.
- 3 For **Description**, enter a brief description of the AP.
- 4 For **Action**, select from the following options:
 - **Report presence only** - When the MAC address of the prohibited AP is detected by an authorized scanning AP, the prohibited AP's presence will be reported in an event message. This in turn will result in the presence of the MAC being included in the Radar threat reports. No countermeasures will be taken against the device with the MAC address by Radar.
 - **Treat like an internal honeypot AP** - The device with the MAC address is considered to be as harmful as an AP that is 'impersonating' one of the authorized APs. If countermeasures are enabled, no devices will be allowed to associate to this MAC address, including devices of other neighboring enterprises.
 - **Treat like an external honeypot** - The device with the entered MAC address is considered to be as harmful as an AP that is advertising a popular SSID. Authorized devices will be prohibited from roaming to the device with this MAC address. Unauthorized devices and unrecognized devices will be allowed to roam to the device with the MAC address.
- 5 Click **Save**. The new access point is displayed in the Prohibited APs list.
For information about reclassifying an existing AP to Prohibited, see .

Reclassifying APs

You can manually assign APs from one category to another depending on the APs current classification. Categorize selected APs directly from its current category list. For example, APs on the Friendly and Uncategorized lists can be reclassified as Authorized.

To reclassify an AP:

- 1 From the top menu, click **Radar**.
- 2 If not already selected, select **Security Analysis Engine** and click **Save**.

- In the left pane, click **Maintenance** and select one of the AP lists. An AP can be reclassified depending on its current classification. See [Table 108](#).

Table 108: AP Classifications

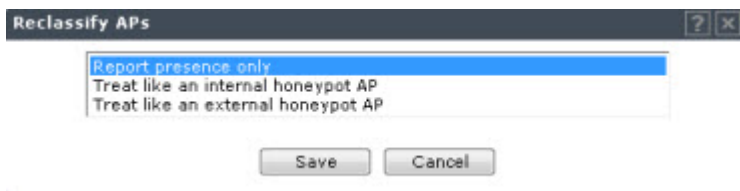
Current AP Category	Possible Reclassification
Friendly	<ul style="list-style-type: none"> Authorized Prohibited
Uncategorized	<ul style="list-style-type: none"> Authorized Friendly Prohibited
Authorized	<ul style="list-style-type: none"> Friendly
Prohibited	<ul style="list-style-type: none"> Friendly

- Select one or more APs from the list and choose an available classification from **Categorize Selected APs as**.
- Click **OK** to reclassify the selected APs.

Reclassifying an AP as a Threat

Friendly and Uncategorized APs can be reclassified as a threat.

- From the **Friendly** or **Uncategorized** AP List, select one or more APs and click **Prohibited**. The **Reclassify APs** dialog displays.

**Figure 148: Reclassify an AP as a Threat**

- Select a threat classification from the list displayed.
- Click **Save**.

Related Links

[Viewing the List of Friendly APs](#) on page 534

[Viewing the List of Uncategorized APs](#) on page 536

Working with Radar Reports

The Analysis Engine receives reports of threats from multiple APs. Different APs can be reporting the same threat incident at the same time. The Analysis Engine needs a way to decide which reports are actually reports of the same threat. It takes a number of factors into account when making this decision. Location is an important attribute used to decide whether two different reports are actually for the same threat.

To view Radar AP reports and statistics:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.

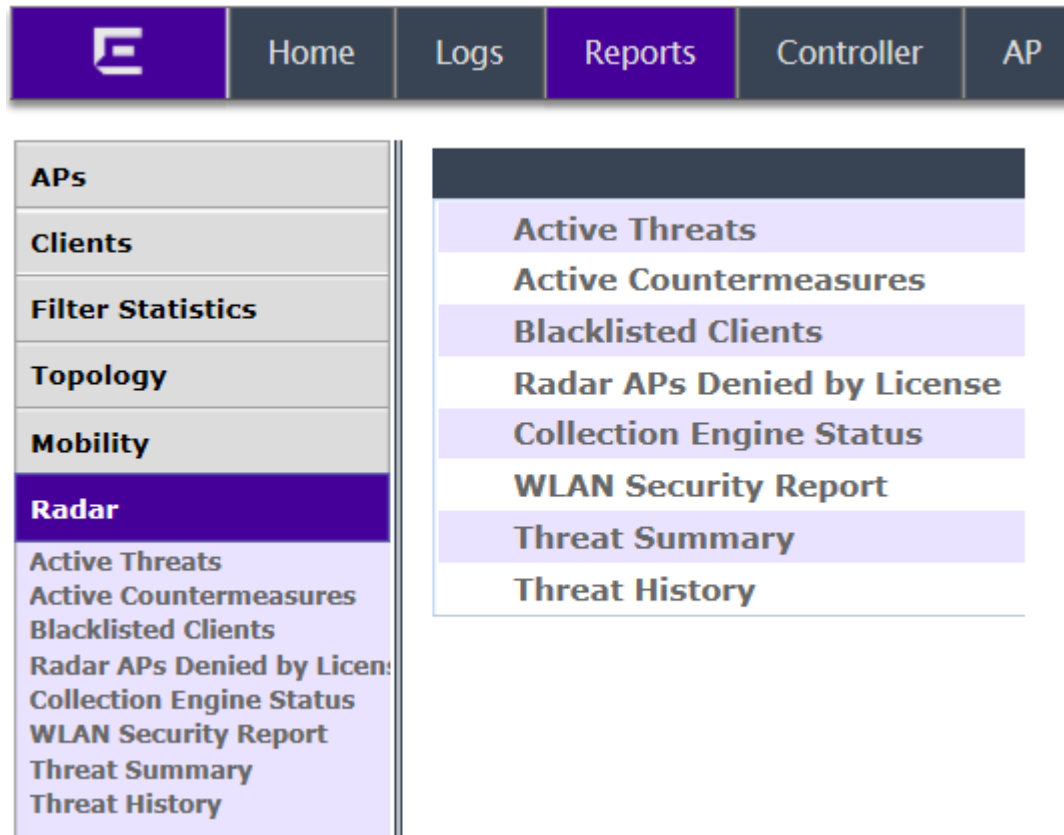


Figure 149: Radar Reports

- 3 Click on the desired report:
 - [Active Threats](#) on page 544
 - [Active Countermeasures](#) on page 546
 - [Blacklisted Clients](#) on page 546
 - [Radar APs Denied by License](#) on page 547
 - [Collection Engine Status](#) on page 548
 - [WLAN Security Report](#) on page 549
 - [Threat Summary](#) on page 550
 - [Threat History](#) on page 552

Security Threats

The Radar reports provide information about security threats. Threat APs are APs that have been detected performing one or more types of attack on the authorized network.

Each AP defined on the controller has a text location attribute that can be set using the controller's GUI, CLI, and SNMP agent. By default the location attribute is empty for all APs. It is strongly recommended that you set the location attribute of each AP. The attribute should be set so that APs at the same location have exactly the same location attribute. For example all the APs on the 3rd floor of a building

could have the same location, such as "Boston/123 4th street/3rd floor". The controller's multi-edit page provides a convenient way to assign groups of APs to the same location.

The types of threat recognized by the Radar WIDS-WIPS system include:

- **Ad Hoc Device** - A device in ad hoc mode can participate in direct device-to-device wireless networks. Devices in ad hoc mode are a security threat because they are prone to leaking information stored on file system shares and bridging to the authorized network.
- **Cracking** - This refers to attempts to crack a password or network passphrase (such as a WPA-PSK). The Chop-Chop attack on WPA-PSK and WEP is an example of an active password cracking attack.
- **Denial of Service (DoS) attacks** - DoS attacks
- **External Honeypot** - An AP that is attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport.
- **Interference Source** - A device that is generating a radio signal that is interfering with the operation of the wireless network. An example of an interference source is a microwave oven which can interfere with 2.4GHz transmissions.
- **Internal Honeypot** - An AP that is attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized network.
- **Roque AP** - A rogue AP is an unauthorized AP connected to the authorized wired or wireless network.
- **Performance** - Performance issues pertain to overload conditions that cause a service impact. Performance issues aren't necessarily security issues but many types of attack do generate performance issues.
- **Prohibited Device** - A MAC address or BSSID is detected that matches an address entered manually into the Radar database.
- **Spoofed AP** - An AP that is not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.
- **Surveillance** - A device or application that is probing for information about the presence and services offered by a network.



Note

Surveillance can be passive (purely listening) or active (surveyor sends messages to speed up the process of surveillance). It is only possible to detect active surveillance. Netstumbler and Wellenreiter are examples of active surveillance tools.

Active Threats

The Active Threats report lists all currently detected threats. Active threats are devices that are being detected performing attacks on the authorized network. Threat APs are identified as APs that have been detected to be performing one or more types of attacks on the authorized network. The report only lists currently active threats, not historic threats. For more information, see [Threat History](#) on page 552.

Viewing Active Threats Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Active Threats**.

Showing 1 to 1 of 1 entries

First Previous 1 Next Last

Search:

Detected Active At	Threat MAC Address	Threat	Threat Category	Countermeasures Applied	Location		Additional Details
					AP Name	RSS	
09/13/2016 06:28:17	FF:FF:FF:FF:FF:FF	Possible attack on WEP or WPA - Excessive frame receive errors	Cracking	No	CS110 - ap3 - AP3825e	N/A	frequency=N/A

Showing 1 to 1 of 1 entries

First Previous 1 Next Last

Figure 150: Active Threats Report

Table 109: Active Threats Report - Fields and Buttons

Field/Button	Description
Detected Active At	Date and time that the threat was identified.
Threat MAC Address	MAC address of the device.
Threat	Type of threat.
Threat Category	For more information, see Security Threats on page 543.
Countermeasures Applied	Indicates if a countermeasure has been applied.
Location - AP Name	Name of the threat AP.
Location - RSS	Threat AP Received Signal Strength (displayed in dBm).
Additional Details	<p>Details of the threat including frequency, SSID, and Rogue Threats. Rogue threats details are accessed by clicking 3 dots “...” that display in the column. The following parameters display in the Rogue Details dialog:</p> <p>Sent MAC address: Sent wireless test packet source MAC address.</p> <p>Received MAC address: Received wired test packet source MAC address.</p> <p>Sent IP address: Wireless test packet source IP address. This IP address is automatically assigned via (DHCP is through the Rogue AP).</p> <p>Received IP address: Wired test packet source IP address.</p> <p>TTL difference: TTL (Time-To-Live or hop limit) difference between sent wireless test packet TTL and received wireless test packet TTL. For example, if the TTL of the sent wireless test packet is 64 and the TTL of the received wireless test packet is 62, then the TTL difference is 2 indicating the packet went through 2 hops.</p> <p>Learned gateway: Wireless gateway IP address as specified from the DHCP server (DHCP is through the Rogue AP).</p>

Modifying the Page's Refresh Rate:

- 1 Type a time (in seconds) in the **Refresh every __ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To add a specific threat to the list of Friendly APs, select the threat and click **Add to Friendly List**.
- 3 To refresh the page, click **Refresh**.
- 4 To export a copy of the report in XML format, click **Export**.
- 5 To close the report window, click **Close**.

Active Countermeasures

The Active Countermeasures report lists each AP currently taking countermeasures. The list also contains the type of attack being countered, when the counter attack started, which channel is being defended, the type of countermeasure in use and when appropriate, the identifiers for the target of the attack.

Viewing Active Countermeasures Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**. The **Available Radar Reports** screen displays.
- 3 Click **Active Countermeasures**. The **Active Countermeasures Report** screen displays.

lab-422-g - Reports - Active countermeasures report No refresh Refresh every secs

Search:

AP Name	AP Serial Number	Started At	Threat MAC Address	Threat Category	Countermeasure
No data available in table					

Data as of Mar 03, 2014 10:25:01 am

Table 110: Active Countermeasures Report - Fields and Buttons

Field/Button	Description
AP Name	Name of the AP taking countermeasures.
AP Serial Number	Serial number of the AP
Threat Category	For more information, see Active Threats on page 544.
Countermeasure	Indicates type of countermeasure applied.
Threat MAC Address	MAC address of the device being countered.
Started At	Date and time that the threat was identified.

Modifying the Page's Refresh Rate:

- 1 Type a time (in seconds) in the **Refresh every __ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To refresh the page, click **Refresh**.
- 3 To export a copy of the report in XML format, click **Export**.
- 4 To close the report window, click **Close**.

Blacklisted Clients

The Blacklisted Clients report lists all devices that are currently on the blacklist (or removed from the whitelist if the list is in whitelist mode) because of the application of countermeasures to an attack.

Clients automatically added to the Blacklist will be removed automatically after the interval configured passes. Station addresses manually added to the Blacklist (or manually removed from the Whitelist) do not appear in this report.

Viewing Blacklisted Clients Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Blacklisted Clients**. The **Blacklisted Clients Report** screen displays.

lab-422-g - Reports - Blacklisted Clients No refresh Refresh every secs

Search:

Blacklisted Address	Blacklisting Started at	Blacklisting Ends at	Reason
No data available in table			

* If whitelisting is used on a controller then blacklisted clients are removed from the whitelist, while they are blacklisted.
If a whitelist grants access to an attacker's address OUI then blacklisting the client has no effect.

Data as of Mar 03, 2014 10:29:14 am

Table 111: Blacklisted Clients Report - Fields and Buttons

Field/Button	Description
Blacklisted Address	MAC address of the blacklisted device.
Blacklisting Started at	Date and time when the device was added to the blacklist.
Blacklisting Ends at	Date and time when the device was removed from the blacklist.
Reason	Reason for blacklisting the device.

To modify the page's refresh rate:

- 1 Type a time (in seconds) in the **Refresh every ___ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To refresh the page, click **Refresh**.
- 3 To export a copy of the report in XML format, click **Export**.
- 4 To close the report window, click **Close**.

Radar APs Denied by License

The Radar APs Denied by License report lists all currently unlicensed APs.

Viewing Radar APs Denied by License Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Radar APs Denied by License**. The following screen displays.

LAB46 - Reports - Radar APs Denied by License No refresh Refresh every secs

Search:

Assigned APs	Scan profile
LAB42-AP3705i	is
LAB46-AP3825i	is

Data as of Oct 02, 2014 04:09:52 pm

Table 112: Radar APs Denied by License Report - Fields and Buttons

Field/Button	Description
Assigned APs	Identifies the name of the assigned Radar APs denied by license.
Scan Profile	Identifies the associated scan profile for the assigned AP.

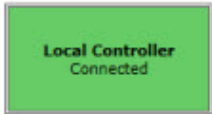
Collection Engine Status

You can view a report on the connection status between the Analysis Engine and the remote data collector engine on each controller.

To View the Collection Engine Status:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, under **Radar**, click **Collection Engine Status**.

lab-422-g - Reports - Collection Engine Status No refresh Refresh every seconds



Data as of Mar 03, 2014 10:31:24 am

The boxes display the IP address of the Data Collector engine. The status of the Data Collector engine is indicated by one of the following colors:

- **Green** — The Analysis Engine has connection with the Data Collector on that controller.
- **Yellow** — The Analysis Engine has connected to the Data Collector but has not synchronized with it. Ensure that the Data Collector is running on the remote controller.
- **Red** — The Analysis Engine is aware of the Data Collector and attempting to connect.

If no box is displayed, the Analysis Engine is not attempting to connect with that Data Collector Engine.



Note

If the box is displayed red and remains red, ensure your IP address is correctly set up to point to an active controller. If the box remains yellow, ensure the Data Collector is running on the remote controller.

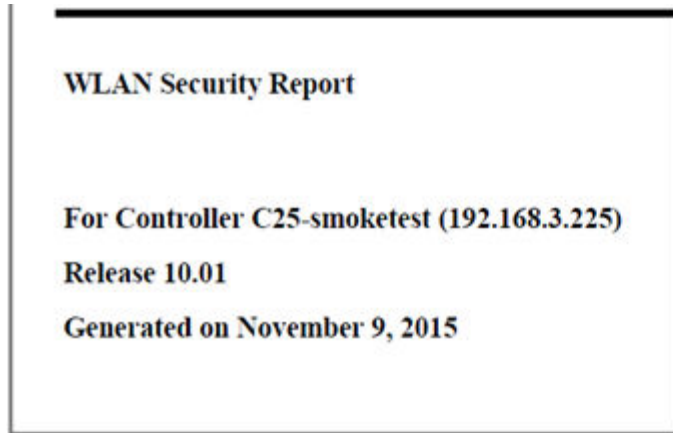
- 1 To modify the page's refresh rate, type a time (in seconds) in the **Refresh every ___ seconds** box at the top of the screen and click **Apply**. The new refresh rate is applied.
- 2 To refresh the page, click **Refresh**.
- 3 To close the report window, click **Close**.

WLAN Security Report

The WLAN Security Report creates a PDF identifying security-related problems in the configuration of the wireless controller WLAN Services. The report identifies issues and provides guidance for their resolution. The report can be printed or saved locally.

Viewing WLAN Security Report Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **WLAN Security Report**.



Report Summary

Introduction

This report identifies security-related problems in the configuration of the controller EWC's WLAN services. The report identifies issues and provides guidance for their resolution.

Issue Summary

Table 1: Counts of WLAN Services and WLAN Services with Issues

	Enabled Services	Disabled Services
WLAN Service	16	3
WLAN Service with Issues	8	1

Distribution of Issues



Figure 151: WLAN Security Report

Threat Summary

The Threat Summary report includes both Active and Historical Threats displayed in the form of pie chart graphs. A device can be counted more than once if it is the source of more than one threat. Each threat category is highlighted using a different color to quickly identify specific threats.

Viewing the Threat Summary

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Threat Summary**. The **Threat Summary** is displayed.

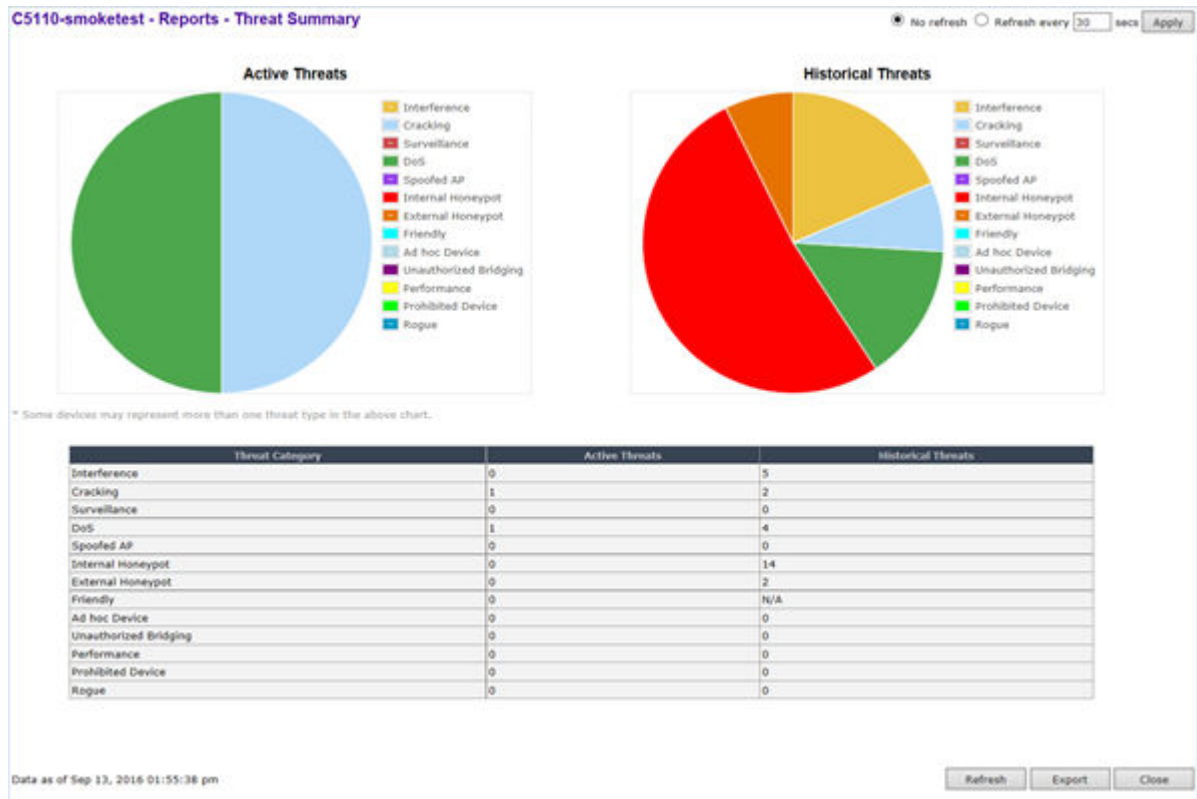


Table 113: Threat Summary Report - Fields and Buttons

Field/Button	Description
Threat Category	List of possible threat categories that are displayed on the summary report. For more information, see Security Threats on page 543.
Active Threats	Total number of active threats identified for each threat category.
Historical Threats	Total number of threats that are no longer active but have been retained on the list for historical tracking purposes. Threats are identified for each threat category.

Modifying the Page's Refresh Rate:

- 1 Type a time (in seconds) in the **Refresh every ___ seconds** box at the top of the screen and click **Apply**.
- 2 To refresh the page, click **Refresh**.
- 3 To export a copy of the report in XML format, click **Export**.
- 4 To close the report window, click **Close**.

Threat History

Viewing the Threat History

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Radar**.
- 3 Click **Threat History**. The **Threat History** screen displays.

C5110-smoketest - Reports - Historical threat report

Showing 1 to 27 of 27 entries

First Previous 1 Next Last Search:

Last Reported	First Detected	Threat MAC Address	Threat	Threat Category	Currently Active	Location		Additional Details
						AP Name	RSS	
09/13/2016 13:58:59	09/13/2016 08:25:41	FF:FF:FF:FF:FF:FF	Null probe response attack	DoS	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=2427
09/13/2016 13:58:17	09/13/2016 04:27:56	FF:FF:FF:FF:FF:FF	Possible attack on WEP or WPA - Excessive frame receive errors	Cracking	Active	C5110 - ap3 - AP3825e	N/A	frequency=N/A
09/13/2016 13:13:05	09/13/2016 12:51:11	FF:FF:FF:FF:FF:FF	Authentication frame flood attack	DoS	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=5785
09/13/2016 12:44:05	09/13/2016 12:39:05	FF:FF:FF:FF:FF:FF	Invalid disconnect code attack	DoS	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=5785
09/13/2016 09:45:19	09/13/2016 05:44:44	N/A	Microwave	Interference	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=2422
09/13/2016 09:44:08	09/13/2016 05:42:01	N/A	Microwave	Interference	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=2417
09/13/2016 09:41:06	09/13/2016 09:40:30	N/A	Video Bridge	Interference	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=2432
09/13/2016 09:41:06	09/13/2016 09:40:50	N/A	Phone	Interference	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=2432
09/13/2016 09:40:46	09/13/2016 09:40:40	N/A	Video Bridge	Interference	Inactive	C5110 - ap3 - AP3825e	N/A	frequency=2427

Table 114: Historical Threat Report - Fields and Buttons

Field/Button	Description
Last Reported	Date and time when the threat was most recently reported.
First Detected	Date and time that the threat was identified.
Threat MAC Address	MAC address of the device.
Threat	Type of threat.
Threat Category	For more information, see Active Threats on page 544.
Currently Active	Current status of the threat.
Location - AP Name	Name of the threat AP.
Location - RSS	Threat AP Received Signal Strength (displayed in dBm).
Additional Details	Detail information on the specific threat.

- 4 To export a copy of the report in XML format, click **Export**.
- 5 To close the report window, click **Close**.

17 Working with Location Engine

Location Engine Overview

Location Engine on the Controller

Deploying APs for Location Aware Services

Configuring the Location Engine

Location Engine Overview

Station location tracking is one of the advanced ExtremeWireless Radar features designed for managing a wireless environment and its resources. The Location Engine works in conjunction with Extreme Management Center maps to define specific floor plan areas for Location Aware Services.

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

Estimating location using readings from multiple APs provides a more accurate location estimate. Estimating location using RSS from a single AP is sufficient to determine the location of client in terms of proximity to the associated AP. The client location is indicated on the map as a circle around the AP. Estimation using multiple RSS offers a pinpoint location estimate of the client. The client location is indicated as a pin, in the most probable position, on the map. The colors displayed around the pin indicate the level of confidence that the client is physically located there.

The Location Engine tracks location of multiple clients simultaneously and returns position relative to the floor plan.

The Location Engine can be configured to track on-demand users, associated users, and unassociated users:

- An on-demand user is a client that is manually added to a preferred list of clients. Space is guaranteed for on-demand users in the Location Engine table. An on-demand user can be either an associated user, such as an employee, or an unassociated user, such as a rogue client that can be tracked as a possible network threat.
- An associated user is an authenticated client. An associated user joins the SSID provided by the AP by simply associating to the open or protected SSID. Location Engine can track location for every associated client up to the controller limit of associated clients.
- An unassociated user is a client that is not authenticated but is in the designated area. Location Engine can track these clients.

No additional license is required to use the Location Engine functionality in the controller. However, to draw maps and to visualize location tracking, Extreme Management Center is required, which comes with its own licensing requirements.

Location Solution Architecture

The ExtremeWireless controller is at the center of the Location Aware Services solution. Location Engine collects RSS reading from APs and displays location data using Extreme Management Center maps or other third-party applications. The following diagram illustrates the solution architecture.

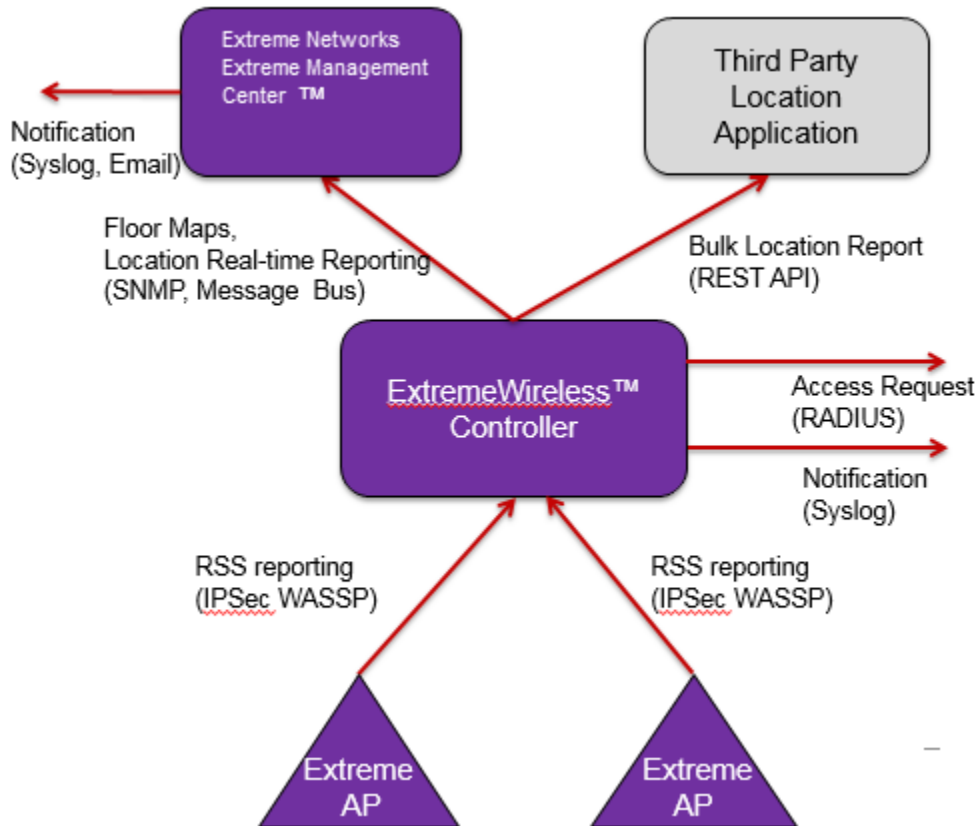


Figure 152: Components of Location Aware Services Solution

Dynamic Filtering

Dynamic filtering is a primary use case for Location Aware Services. This feature controls client access based on location. Customers can use Location Aware Services in schools and hospitals to define access parameters within a designated area. This functionality combined with the role assignment from Network Access Control (NAC), makes it possible to implement dynamic filtering on the client location. Network access rights (access to servers or applications) can depend on the client location -- inside or outside the defined area. Role assignment is accomplished dynamically by the controller and NAC as client moves within the floor plan.

Bulk Reporting

Location Engine can export bulk reporting data for use in third-party applications. For example, use Location Engine data to determine traffic flow in large venues and time-of-use analytics. The controller's bulk reporting data includes location of the client, the serial number of the associated AP,

the name of the floor plan, and more. Third-party location client applications can synchronize their floor maps directly from the controller (either on-demand or on a scheduled basis using the controller CLI).

Although it is possible to access the Location Engine data directly using a CLI session, most users will choose to access location data using Extreme Management Center maps or a third-party location client application.

Location Engine on the Controller

Location Engine tracks location of multiple clients simultaneously and returns position relative to the floor plan. The following are components of the Location Engine:

- **Heat Map.** The Location Engine generates a heat map of each AP on a user-provided floor plan. The Location Engine analyzes the floor plan and considers the presence and material of structures or obstacles, such as walls, when calculating the predictive coverage map.

Extreme Management Center™ is required to define the floor plan. Be sure to include the presence of walls and obstacles when defining the floor plan. For information about defining a floor plan, see the *Extreme Management Center™ User Guide*.

- **Localization algorithms.** Location Engine algorithms scan all APs that report the client and select RSS readings from three or more APs that are most likely to provide the best location estimates. Using the selected RSS readings, location is triangulated and returned as the Cartesian coordinates relative to the floor plan.
- **Notification.** Location is reported immediately on a real-time stream and as a notification on the event stream (syslog). The controller tracks the client location and can determine when a client is inside a predefined area. You can define up to 16 areas of interest per floor map using Extreme Management Center. The Location Engine offers a Track Area Change feature, that, when enabled, triggers a notification each time a client moves from one area to another. The notification events can be used for improved radio resource management such as Network Access Control (NAC). For information about how to enable Track Area Change, see [Configuring the Location Engine](#) on page 557.
- **Simultaneous updates.** Location Engine simultaneously updates the location of tracked clients. It can track the number of clients that can be supported by the controller. If the controller is part of an availability pair, it can also track the clients supported by the availability partner, and Location Engine is not restricted by floor size.

Client location is presented in Extreme Management Center. [Figure 153](#) illustrates a blue pin placed on the most probable position of the client. The map is colored according to the expected probability of the client position. Black is the most likely and yellow is the least likely position.

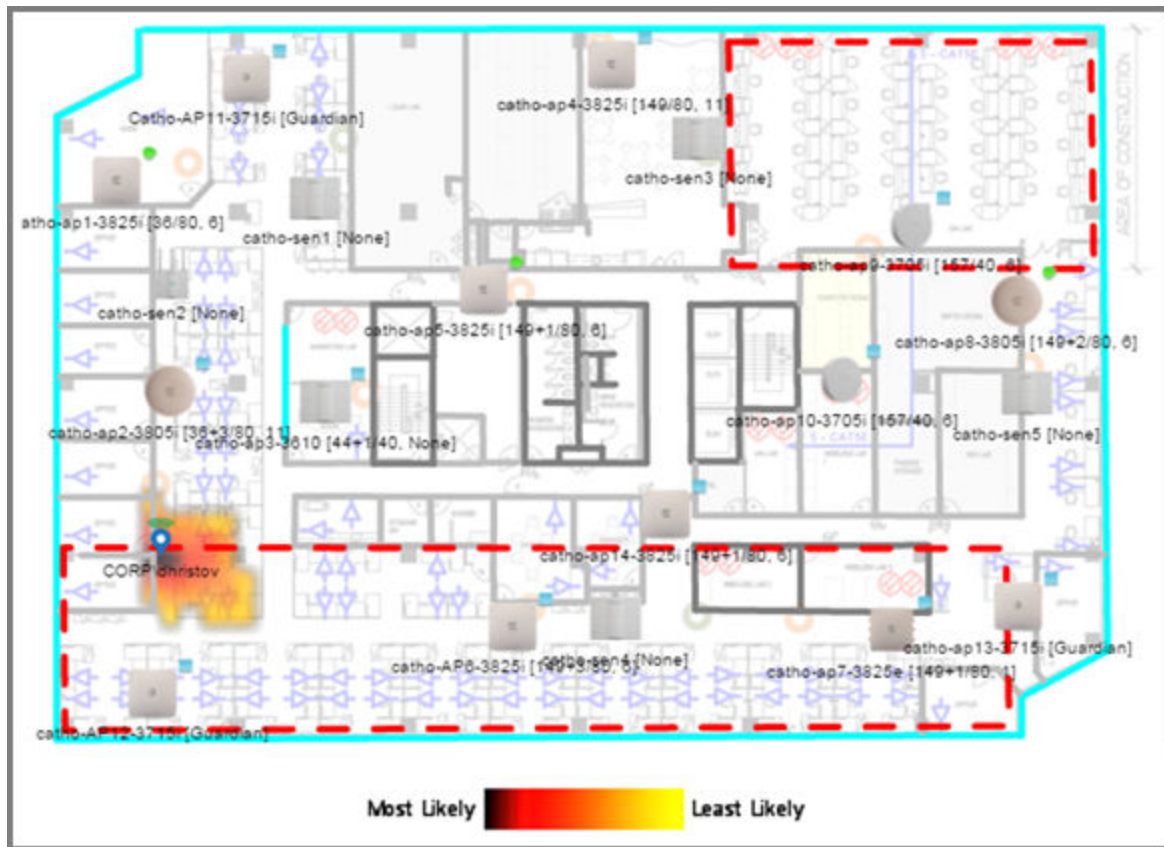
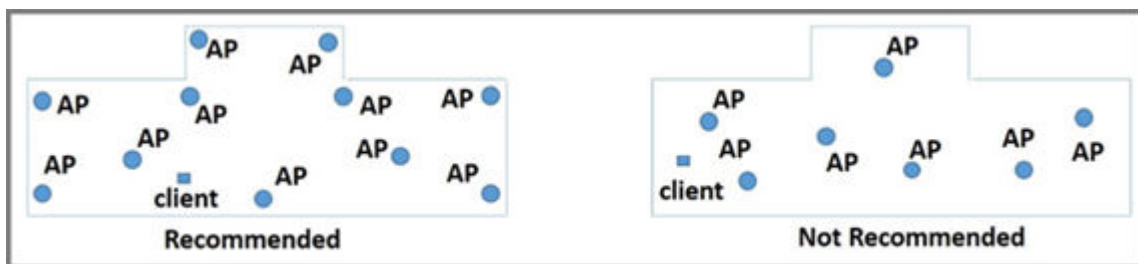


Figure 153: Extreme Management Center Floor Plan

Deploying APs for Location Aware Services

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

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



- The maximum distance between APs depends on environmental factors such as the presence of walls and structures, but as rule of thumb, in a location aware deployment, place the APs 10 to 20 meters apart.
- Install APs at the same height on the wall, and do not install APs behind walls or ceilings.
- Install APs away from metal structures like poles or racks, because metal can affect the radiated pattern.
- When location accuracy is paramount, augment your in-service deployment with Guardian APs. Guardian APs scan multiple channels where in-service APs operate on a single channel. Therefore, Guardian APs are capable of registering readings from more clients than in-service APs. Guardian APs also increase the number of triangulation points. The Guardian mitigates the problem of non-probing clients and is capable of sensing a client based on the data packets. For more information, see [Configuring an AP as a Guardian](#) on page 195.

Configuring the Location Engine

Location Engine configuration involves defining environmental factors in the floor plan, location targets, area change notification, and client targets. The following information is provided to help you configure the Location Engine:

- [Enabling the Location Engine](#) on page 557
- [Location Batch and Client Reporting](#) on page 559
- [Creating a New Destination URL](#) on page 560
- [Creating a New On-Demand User](#) on page 561
- [Downloading a Floor File](#) on page 561
- [Uploading an Existing Floor File](#) on page 563
- [Deleting a Floor Plan](#) on page 564

Enabling the Location Engine

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.

- 3 To Enable/Disable the Location Engine, select or clear the **Location Engine** checkbox.

Table 115: Location Engine Settings Dialog - Fields and Buttons

Field/Button	Description
Environment Settings	
Default AP Height (cm)	Enter the height of the AP based on its location on the wall.
Default Environmental Model	Select a mode that best matches the environment identified by the floor plan. Choose from one of the following modes from the drop-down list: <ul style="list-style-type: none"> Indoor open space (halls, auditoriums) Office Environment with light divisions (cubicles) Office Environment with dry wall divisions Office Environment with hard divisions (brick) Interior Walls (need be defined in the floor plan)
None	Locator does not collect or triangulate RSS readings.
Clients	Locator tracks active sessions only.

Table 115: Location Engine Settings Dialog - Fields and Buttons (continued)

Field/Button	Description
All	Locates all active users and all non-associated users (MAC) around deployed APs located within the signal range. RSS readings from non-associated users are included in the Location Engine table. Note: The Location Engine table is shared between all tracked users. This table does not increase in size and does not reserve space for associated users. Once the number of tracked users exceeds the limit, additional users will not be added to the table. Users remain in the table until they time out. Users designated as On-Demand are guaranteed space in the Location Engine table.
Track Area Change	The controller tracks the client location and can determine when a client is inside a predefined area. Select Track Area Change to trigger a notification when a client moves from one area to another. Use the notification events to improve radio resource management such as Network Access Control (NAC).
On-Demand Users	Displays a list of known MAC addresses present in the area, for example, a list of employees. On-demand users are guaranteed space in the Location Engine table.
Add	Click to create a new on-demand user. For more information, see Creating a New On-Demand User on page 561
Delete Selected	Click to delete the selected on-demand user.
Advanced	Click to open the Advanced dialog, which lists available floor plans. From the Advanced dialog, you can upload and download floor plans. For more information, see Downloading a Floor File on page 561
Save	Click to save changes.

Location Batch and Client Reporting

When the Location Engine is enabled and configured to publish locations, it posts location data in XML format to a given location. The location data is pushed to up to five given destinations periodically within the given time interval. Batch reporting continues until Location Batch Reporting is disabled, the Location Engine is disabled, or the controller is powered off.

In location-based applications and user traffic analytics, integrating partners often require more detail than simply the location of a MAC address. The client reporting option allows users to generate a report with details from the MU-Table.

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Location Engine**.
- 3 To enable/disable the Location Batch Reporting, in the left pane, select **Location Batch Reporting** then select the **Location Batch Reporting** checkbox.
- 4 To enable/disable the Client Reporting, in the left pane, select **Location Batch Reporting** then select the **Clients Detail Reporting** checkbox.

Location Batch Reporting

Clients Detail Reporting

Report every minute(s)

Dimension Unit

Post all location destinations to the following URLs:

	Login	Password	Destination URL
<input type="checkbox"/>	1	*	http://1.1.1.1
<input type="checkbox"/>	2	*****	http://1.1.1.2
<input type="checkbox"/>	3	*****	http://1.1.1.121

Figure 154: Reporting Options

Table 116: Location Batch and Client Detail Reporting Fields and Buttons

Field/Button	Description
Report all station locations every (X) minutes	Select a time (in minutes) for station reporting from the drop-down list.
Dimension Unit	Select a dimension unit, from the drop-down list, for measuring location destinations. (Displayed for Location Batch Reporting only.)
Login	Login ID of the destination URL.
Password	Password of the destination URL.
Destination URL	List of destination URLs.
Add	Click to create a new Destination URL. For more information, see Creating a New Destination URL on page 560.
Delete Selected	Click to delete the selected Destination.
Save	Click to save changes.

Creating a New Destination URL

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

- 2 In the left pane, click **Location Engine** > **Location Batch Reporting** and select either **Location Batch Reporting** or **Client Detail Reporting**.
- 3 Click **Add**. The **Destination URL** dialog displays.

The screenshot shows a dialog box titled "Destination URL". It has a dark header bar with a question mark icon and a close button (X). The main area contains three text input fields: "Login:", "Password:", and "Destination URL:". Below the fields are two buttons: "OK" and "Cancel".

- 4 Enter a user ID and password for the destination URL.
- 5 Enter a URL for the new destination.
- 6 Click **OK**.

Creating a New On-Demand User

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.
- 3 Click **Add**. The **On-demand User** dialog displays.

The screenshot shows a dialog box titled "On-demand User". It has a dark header bar with a question mark icon and a close button (X). The main area contains one text input field labeled "MAC Address:". Below the field are two buttons: "OK" and "Cancel".

- 4 Enter a MAC Address for the new on-demand user.
- 5 Click **OK**.

Downloading a Floor File

The **Download** button is always enabled. All information about the floor pan is contained in the file being downloaded including unique identifiers for the floor plan.

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.

- 3 Click **Advanced**. The **Advanced** dialog displays.

Advanced

Show 10 entries Search:

Floor ID	Floor Name	Number of APs	Cell Size	Floor Size			Type of Environment
				Number of Cells	Width	Length	
1	Thornhill	9	100X100	2035	3700	5500	Model 4

Showing 1 to 1 of 1 entries

Download... Upload Selected... Delete Selected...

¹ To sort by multiple columns, click the first column, hold down the SHIFT key, and then click the next column. As many columns as you wish can be added to the sort.

Close

- 4 Click **Download**. The **Download and Import Floor Plan File** dialog displays.

Download and Import Floor Plan File

Protocol: FTP

Server:

User ID:

Password:

Confirm:

Directory:

Filename:

Download

Close

Table 117: Download and Import Floor File Dialog - Fields and Buttons

Field/Button	Description
Protocol	Select the transfer protocol from one of the following: <ul style="list-style-type: none"> • FTP • SCP
Server	IP address of the server containing the floor file.
User ID	Required ID to access the server.
Password	Password required for access to the server.
Confirm	Enter the password for confirmation
Directory	Location of the floor file on the selected server
Filename	File name of the floor plan file on the selected server.

- 5 Click **Download** to import the floor plan, or click **Close** to cancel the import.

Uploading an Existing Floor File

The Upload Selected button is enabled when a row within the list of floor plans is highlighted.

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Location Engine**. The Location Engine Settings screen displays.
- 3 Click **Advanced**. The **Advanced** dialog displays.

The screenshot shows the 'Advanced' dialog box with a table of floor plans. The table has columns for Floor ID, Floor Name, Number of APs, Cell Size, Floor Size (Number of Cells, Width, Length), and Type of Environment. A single row is highlighted, representing a floor plan with ID 1, name Thornhill, 9 APs, 100X100 cell size, 2035 cells, 3700 width, 5500 length, and Model 4 environment.

Floor ID	Floor Name	Number of APs	Cell Size	Floor Size			Type of Environment
				Number of Cells	Width	Length	
1	Thornhill	9	100X100	2035	3700	5500	Model 4

Buttons at the bottom include 'Download...', 'Upload Selected...', 'Delete Selected...', and 'Close'. A search bar and 'Show 10 entries' are also visible.

¹ To sort by multiple columns, click the first column, hold down the SHIFT key, and then click the next column. As many columns as you wish can be added to the sort.

- 4 Select a floor file from the list of floor files.

- Click **Upload Selected**. The Upload Floor Plan File dialog displays.

Table 118: Upload Floor Plan File Dialog - Fields and Buttons

Field/Button	Description
Protocol	Select the transfer protocol from one of the following: <ul style="list-style-type: none"> • FTP • SCP
Server	IP address of the server where the file will be exported.
User ID	Required ID to access the server.
Password	Password required for access to the server.
Confirm	Enter the password for confirmation
Directory	Location of the floor file directory on the destination server.
Filename	File name of the floor plan file on the destination server.

- Click **Upload** to export the floor plan, or click **Close** to cancel the export.

Deleting a Floor Plan

- From the top menu, click **Radar**.
- In the left pane, click **Location Engine**. The **Location Engine Settings** screen displays.
- Click **Advanced**. The **Advanced** dialog displays.

Advanced ? X

Show entries Search:

Floor ID	Floor Name	Number of APs	Cell Size	Floor Size			Type of Environment	
				Number of Cells	Width	Length		
1	1	Thornhill	9	100X100	2035	3700	5500	Model 4

Showing 1 to 1 of 1 entries ◀ ▶

¹ To sort by multiple columns, click the first column, hold down the SHIFT key, and then click the next column. As many columns as you wish can be added to the sort.

- 4 Select a floor file from the list of floor files. Only one floor file can be deleted at a time.
- 5 Click **Delete Selected** to delete the floor file from the list. Click **OK** to confirm the delete operation.
- 6 Click **Close**.

18 Working with Reports and Statistics

Application Visibility and Device ID
Viewing AP Reports and Statistics
Viewing All Clients
Viewing Role Filter Statistics
Viewing Topology Reports
Viewing Mobility Reports
Viewing Controller Status Information
Viewing Routing Protocol Reports
Viewing RADIUS Reports
Call Detail Records (CDRs)

This chapter describes the various reports and statistics available in the Wireless system including:

- Viewing AP Reports and Statistics
- Viewing Active Clients
- Viewing Role Filter Statistics
- Viewing Topology Reports
- Viewing Mobility Reports
- Viewing Controller Status Information
- Viewing Routing Protocol Reports
- Call Detail Records (CDRs)
- Application Visibility and Device Identification

Application Visibility and Device ID

With ExtremeWireless, you can identify devices and applications on the wireless network. From the dashboard and the Active Client report, you can view:

- 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.

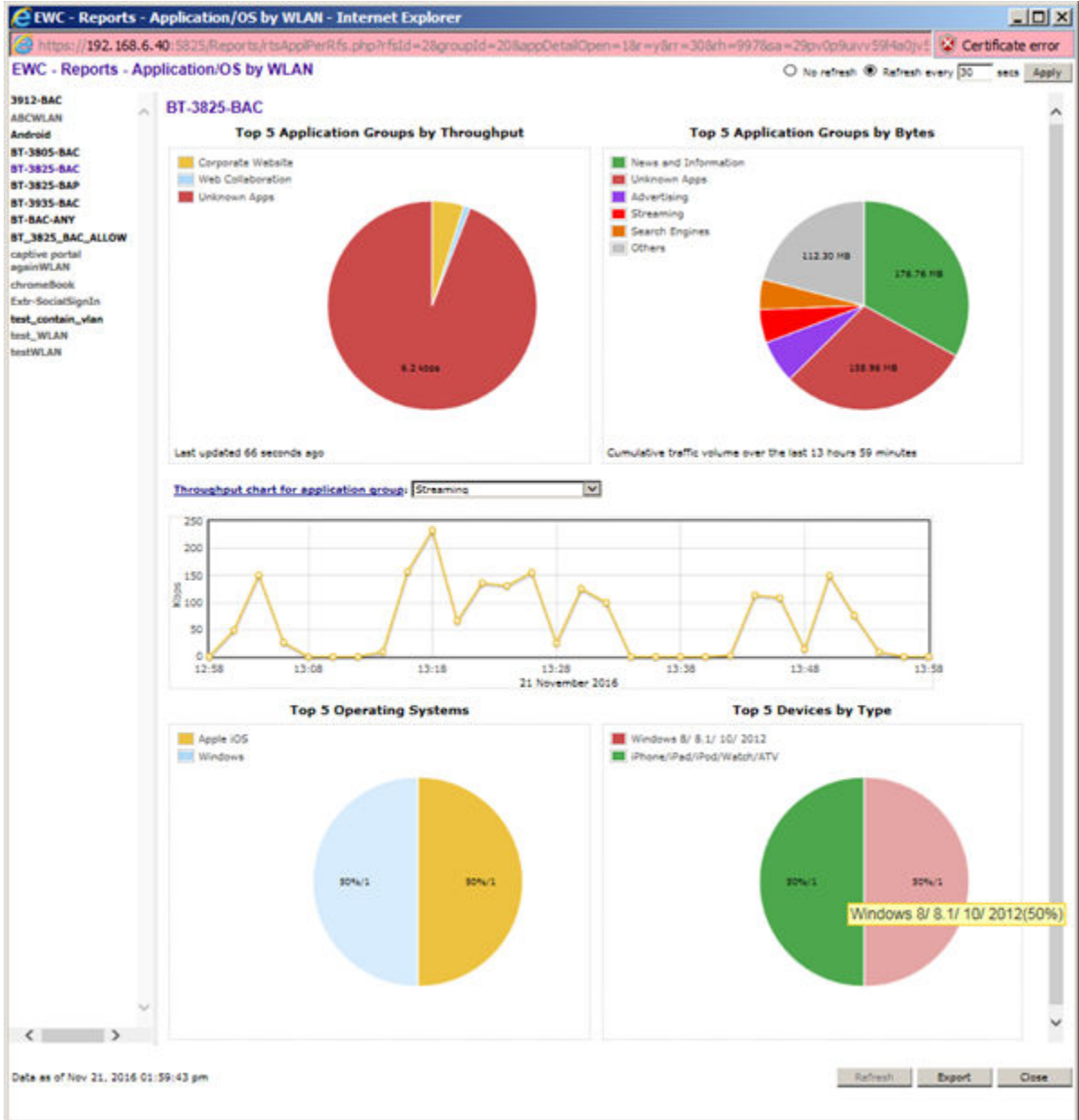


Figure 155: Application Visibility by WLAN

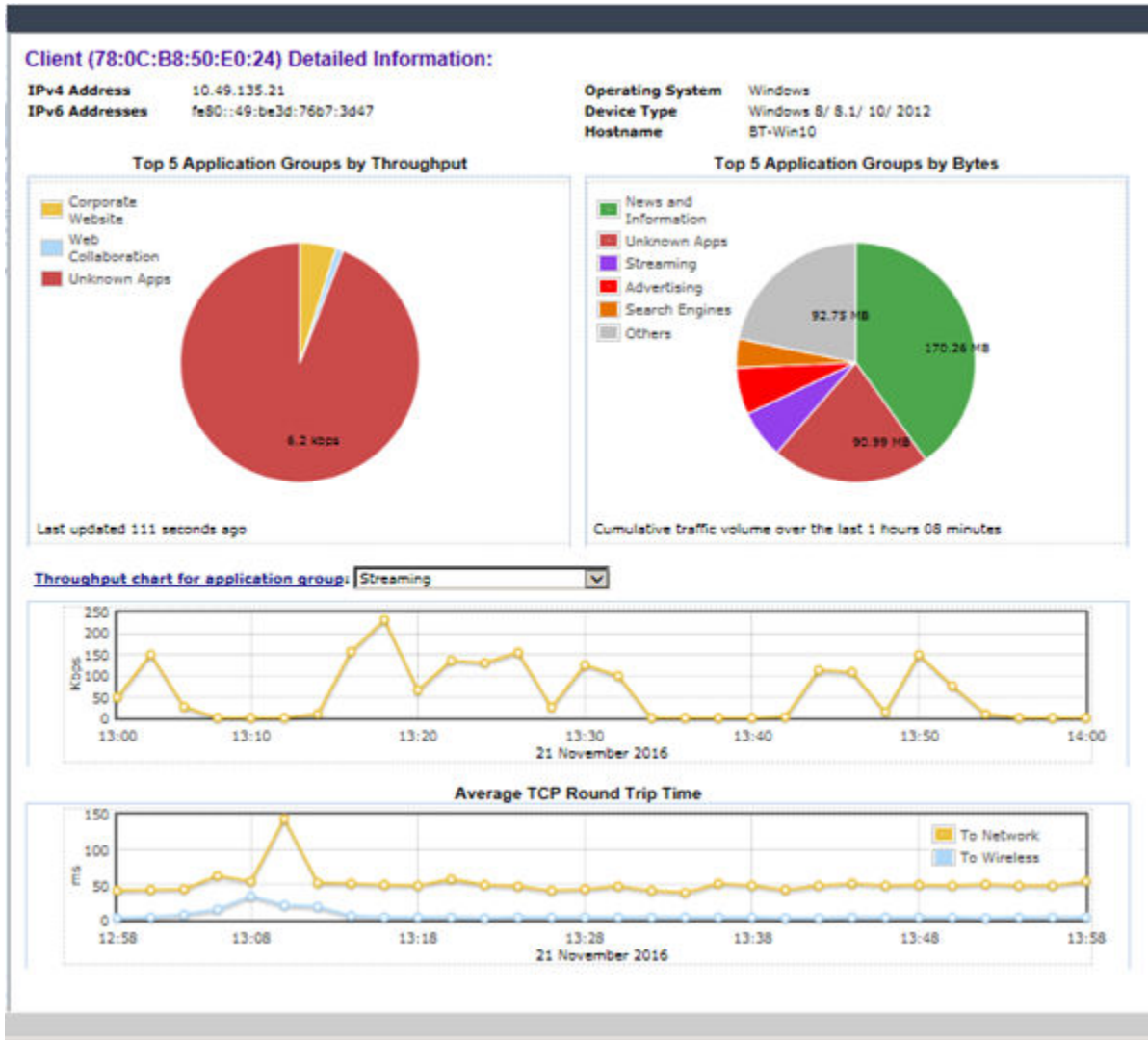


Figure 156: Application Visibility by Client

Related Links

- [Application Visibility](#) on page 568
- [Device Identification](#) on page 570
- [Enabling Application Visibility with Device Identification](#) on page 571
- [Displaying Client Details](#) on page 588
- [Wireless Assistant Home Screen](#) on page 36

Application Visibility

With the ability to gather application analytics, you can engineer wireless traffic to support company policies, preserve bandwidth, identify critical applications, assign higher priority and QoS values, and enhance network security. Application Visibility and Application Enforcement makes it possible to block restricted web content and block or limit peer-to-peer protocols to preserve network bandwidth.

With ExtremeWireless, you can view the top 5 application groups by WLAN from the controller Home dashboard and the top 5 application groups for each client from the [Client Details report](#).

The **Applications by WLAN** pie chart displays the top 5 application groups running on that WLAN. ExtremeWireless cycles through the active WLANS displaying statistics. To view detailed statistics, enable Application Visibility during the WLAN configuration; then, on the Home dashboard, click the displayed pie chart under **Applications by WLAN**. Or, click **Enable Application Visibility** from the Home dashboard.

The controller and AP capture statistics for 31 pre-selected application groups. The top 5 application groups are displayed based on bytes and throughput over the last two-minute measuring period. The stats for each WLAN display for 30 seconds on a continuous cycle. Historical statistical data is available from ExtremeCloud™ and Extreme Application Analytics™.

To manage wireless traffic in support of company policies, define Layer 7 filter rules from the **Filter Rule Definition** dialog. Layer 7 represents the application layer of the OSI communication module. Define policy rules with access control actions for specific applications or groups of applications. Application visibility supports standard Extreme Application Analytics™ signatures. You can also configure up to 64 extended web application signatures.

**Note**

For application enforcement, you must enable Application Visibility in WLAN configuration.

Related Links

[L7 Configuration](#) on page 262

[Application Visibility and Device ID](#) on page 566

[Device Identification](#) on page 570

[Wireless Assistant Home Screen](#) on page 36

[Enabling Application Visibility with Device Identification](#) on page 571

Application Control for Tunneled Traffic

To classify a flow, the DPI engine must examine both client and server packets. The controller enforces policy for downstream traffic and the AP enforces policy for upstream traffic. For tunnel traffic, the DPI engine must examine the packets at the controller. Enforce this by clearing the **AP Filtering** checkbox on the Policy Rules tab.

Role: anUnauth

VLAN & Class of Service **Policy Rules**

Inherit filter rules from currently applied role i

Rules AP Filtering

In	Out	EthType	MAC	IP : Port	Protocol
dest	src	0x0800	Any	172.16.209.1/32	Any
dest	src	0x0800	Any	192.168.11.22/32	Any
dest	src	0x0800	Any	0.0.0.0/0:67 (DHCP S	UDP
dest	none	0x0800	Any	0.0.0.0/0	Any
none	src	0x0800	Any	0.0.0.0/0	Any

Figure 157: Configuring Policy Rules for Downstream Traffic at the Controller

Device Identification

ExtremeWireless can identify the device type and operating system used by clients associated with an ExtremeWireless AP. Gathering this information in a site deployment furthers mobile user statistical reporting on the controller or Cloud. This feature is supported on the ExtremeWireless AP38xx or AP39xx series APs. This discovery is implemented on the AP through deep packet inspection of the and HTTP packets. Regardless of how the traffic is bridged -- at the controller or routed -- fingerprinting is handled on the AP. This approach offers a consistent implementation that does not require a large processing load. The AP fingerprints the same messages as Extreme Access Control.

Device ID is based on a DHCP database. The database is defined by an XML file that is built into both the AP and controller image. The XML file can be updated each time the image file is updated.

The precision of the client's identity improves overtime. Each DHCP fingerprint has an assigned weight in the XML file. HTTP fingerprints are assigned a greater weight than DHCP fingerprints. The AP tracks the weight of a client's fingerprint. If a client is identified with a fingerprint that has a greater weight than what was previously stored in the database, the new device identity and weight value are updated in the database.

The AP reports device identity changes to the controller and to the Cloud. This information is available to the user through the ExtremeWireless dashboard and through the controller reporting system. The client device type is included in all data streams where client parameters are included. For instance, this information is available to the ExtremeWireless Location Engine and to Extreme Management Center™.

Related Links

[Application Visibility and Device ID](#) on page 566

[Wireless Assistant Home Screen](#) on page 36

[Displaying Client Details](#) on page 588

Enabling Application Visibility with Device Identification

To view statistics on the applications and devices associated with a specific WLAN, configure the WLAN with Application Visibility enabled. You can enable visibility from the **WLAN configuration** screen or temporarily enable visibility from the **Home** screen dashboard.

To enable Application Visibility from the WLANs:

- 1 Go to **VNS > WLAN Services** and select a WLAN or click **New**.

The screenshot shows the configuration page for a WLAN named 'Lab126-13-AAA'. The 'WLAN Services' tab is active. Under the 'Core' section, the 'App Visibility' checkbox is checked and highlighted with a red box. Other settings include: Name: Lab126-13-AAA, Service Type: Standard, SSID: Lab126-13-AAAMF5, Default Topology: -, Default CoS: No CoS, and Default Traffic Mirror: Prohibited. The 'Status' section shows the 'Enable' checkbox is also checked. The left sidebar shows a list of WLAN services, with 'Lab126-13-AAA' selected.

Figure 158: Application Visibility Check box Option

- 2 Check the **App Visibility** option and click **Save**.



Note

You can enable Application Visibility from the Home dashboard for WLANs that do not have this configuration option enabled.

Related Links

[Application Visibility](#) on page 568

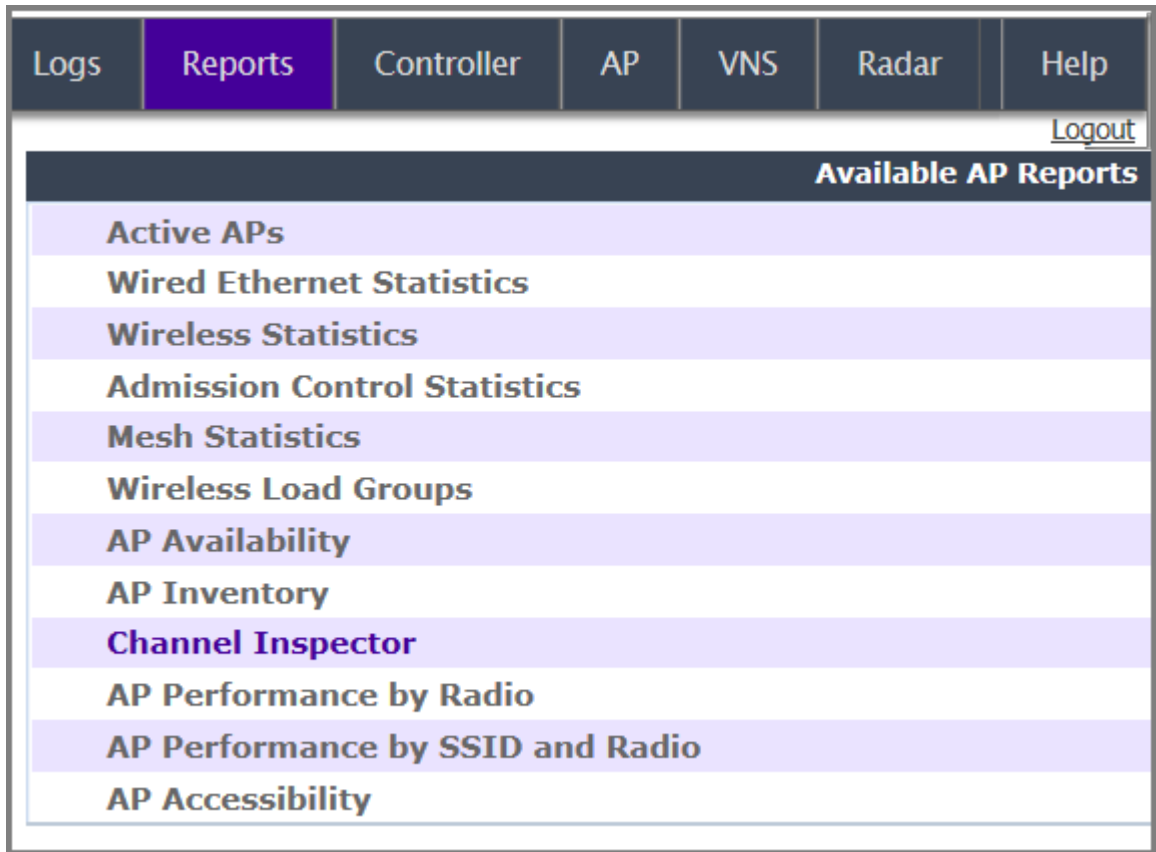
[Device Identification](#) on page 570

[Wireless Assistant Home Screen](#) on page 36

Viewing AP Reports and Statistics

To view AP reports:

From the top menu, click **Reports**.



Viewing Statistics for APs

Several displays are snapshots of activity at that point in time on available APs:

- Active APs
- Wired Ethernet Statistics
- Wireless Statistics
- Admission Control Statistics
- Mesh Statistics
- Wireless Load Groups
- AP Availability
- AP Inventory
- Channel Inspector
- AP Performance by Radio
- AP Performance by SSID and Radio

- AP Accessibility
- AP Dashboard. See [AP Dashboard](#) on page 148

The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

Viewing Active Wireless APs

Statistics in the **Active Wireless APs** report are expressed in respect to the AP. For example, Packets Sent indicates the packets the AP has sent to a client and Packets Rec'd indicates the packets the AP has received from a client.

- 1 From the top menu, click **Reports**.
- 2 Click the **Active APs** display option. The **Active Wireless APs** display opens in a new browser window.

Wireless AP	Serial	AP IP	Client	Role	Mesh/WDS Child	Sec. Tunnel	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	Captures	Invalid Rate	Radio 1 Mode	Radio 1 Ch	Radio 1 PM	Radio 2 Mode	Radio 2 Ch	Radio 2 PM
CS110-421-4F3765e	000000VFA1472019	10.218.0.33.0		Local Traffic Forwarder 0 (AP)		N/A	4:32:28	7373	12914	363144	1267424	4:33:48	off	0	off	off	-	off	off	-
CS110-423-4F3825e	1418824298940000	10.218.0.15.0		Local Traffic Forwarder 0 (AP)		N/A	4:33:27	7397	13067	673816	1347693	4:33:43	off	0	off	off	-	off	off	-

Necessary 2 active APs

¹ Channel selection in progress
² DFS Timeout
³ Number of active immediate Mesh/WDS child APs
⁴ S: Secure tunnel; C: Secure tunnel control encryption; D: Secure tunnel data encryption

Data as of Nov 10, 2015 01:10:39 pm

Viewing Wired Ethernet Statistics:

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.
- 2 Click the **Wired Ethernet Statistics** display option. The **Wired Ethernet Statistics by Wireless APs** display opens in a new browser window.

Status	IP Address	MAC Address	MTU Interface	MTU Tunnel
Approved	134.141.121.228	D8:04:66:74:FF:7B	1500	1500

Up Link

Statistics	Sent	Received
Discarded Packets	0	2
Total Errors	0	0
Unicast Packets	8168150	12249770
Multicast Packets	263826	8109836
Broadcast Packets	18923	984002
Total Packets	8459899	21343608
Total Bytes	2657349764	12668845861

Client Ports

Statistics	p1		p2		p3	
	Sent	Received	Sent	Received	Sent	Received
Discarded Packets	0	0	0	0	0	0
Total Errors	0	0	0	0	0	0
Unicast Packets	0	0	0	0	0	0
Multicast Packets	0	0	0	0	0	0
Broadcast Packets	0	0	0	0	0	0
Total Packets	0	0	0	0	0	0
Total Bytes	0	0	0	0	0	0

Data as of Jan 25, 2017 03:40:49 pm

- 3 In the left pane, click a registered AP to display its information.

Viewing Wireless Statistics:

- 1 From the top menu, click **Reports**.
- 2 Click the **Wireless Statistics** display option. The **Wireless Statistics by Wireless APs** display opens in a new browser window.

lab-422-g - Reports - Wireless Statistics by Wireless APs No refresh Refresh every secs

C4110 - ap1 - AP4102
C4110 - ap2 - AP3620

AP Status: Approved
AP IP Address: 10.219.40.10

Radio1		Radio2	
MAC Address	00:11:88:38:47:80 00:11:88:38:47:81 00:11:88:38:47:82 00:11:88:38:47:83 00:11:88:38:47:84 00:11:88:38:47:85 00:11:88:38:47:86 00:11:88:38:47:87	Mode	a
SSID	CNL-422-1-7-ssid CNL-422-1-6-ssid CNL-422-1-5-ssid CNL-422-0-3-ssid CNL-422-0-2-ssid CNL-422-0-1-ssid CNL-422-0-0-ssid CNL-422-WDS-ssid	Channel	157
		Current Power Level	10 dBm
		Operational Max Rate	54 Mbps

Associated Clients There are no active clients on this radio

Active immediate WDS child APs 1

Statistics	Sent	Received
Discarded Packets	49	286
Errors	49	221413
Unicast Packets	1251293	290501
Multicast Packets	0	2038

Data as of Mar 03, 2014 10:55:24 am

- 3 In the **Wireless Statistics by Wireless APs** display, click a registered AP to display its information.
- 4 Click the appropriate tab to display information for each Radio on the AP.

Viewing Admission Control Statistics by Wireless AP:

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

- Click the **Admission Control Statistics** display option. The **Admission Control Statistics by Wireless AP** display opens in a new browser window.

lab-422-g - Reports - Admission Control Statistics by Wireless AP

Users: C4110 - ap1 - AP4102 0
C4110 - ap2 - AP3620 1

C4110 - ap1 - AP4102 0002000609223321

Client IP	Client MAC	Protocol	BSS MAC	SSID	AC	Direction	MDR [bps]	NMS [bytes]	SBA	Rate [bps]		Violations [bps]	
										DL	UL	DL	UL
No Client is connected to this Wireless AP													

Active Users: 1 Search Client by user name Search

- In the **Admission Control Statistics by Wireless AP** display, click a registered AP to display its information:
- The **Admission Control Statistics by Wireless AP** lists the TSPEC statistics associated with this AP:
 - AC** — Access class where TSPEC is applied,
 - Direction** — Inbound, Outbound or Bidirectional,
 - MDR** — Mean Data Rate
 - NMS** — Nominal Packet Size
 - SBA** — Surplus Bandwidth (ratio)

The following statistics are of measured traffic:

 - Rate** — Rate in 30 second intervals (inbound and outbound)
 - Violation** — Number of bits in excess in the last 30 seconds (inbound and outbound)

Viewing Mesh VNS Wireless AP Statistics:

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

- From the Available AP Reports screen, click **Mesh Statistics**. The **Mesh Statistics** display opens in a new browser window.

lab-422-g - Reports - Mesh Statistics

No refresh Refresh every secs

AP Name	SSID	Rx Rss	Hops	Rx/Tx Rate	Backhaul Channel	Parent Change	Rx Frames	Tx Frames	Rx/Tx Errors	Retry Percent
C4110 - ap1 - AP4102[MP]	N/A	N/A	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A
C4110 - ap2 - AP3620	CNL-422-WDS-ssid	-52	1	54/54	157: (5785)	2	393988	223782	0/2	5

Data as of Mar 03, 2014 10:59:02 am

The Rx RSS value on the Mesh Statistics display represents the received signal strength (in dBm).

Viewing Load Balance Group Statistics

The **Active Wireless Load Groups** report lists all load groups, and for the selected load group, all active AP radios.

To View the Active Wireless Load Groups Report:

- From the top menu, click **Reports**.
- Click the **Wireless Load Groups** report.

The **Active Wireless Load Groups** report opens in a new browser window. Reports display differently when reporting on client balance load groups and radio preference load groups.

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
CNL-208-C20-1						
Members				4		
Clients				0		
Average Load				0.0		
0500008043050356	1	0	Under-Loaded	0	0	0
0500008043050356	2	0	Under-Loaded	0	0	0
10490056235A0000	1	0	Under-Loaded	0	0	0
10490056235A0000	2	0	Under-Loaded	0	0	0
Members: 4 Clients: 0 Average Load: 0.0						

About Radio Preference/Load Control Statistics

The statistics reported for each radio preference load balance group are:

- Members** — The number of AP members

The statistics reported for each member of the load balance group are:

- AP** — AP name

- **Band Preference**
 - **Status** —The operational status: enabled or disabled
 - **Probes Declined** —The number of probes declined
 - **Auth/Assoc Requests Declined** —The number of authentications or associations declined
- **Load Control**
 - **Radio 1**
 - Status** —The operational status: enabled or disable
 - Rejected** —The number of clients declined at the first association attempt
 - **Radio 2**
 - Status** —The operational status: enabled or disabled
 - Rejected** —The number of clients declined at the first association attempt
 - Returned** —The number of clients declined at the second association attempt

Load balance group statistics are reported on the foreign controller when APs fail over with load groups from a different controller indicated with an “(F)” following the load group name.

About Client Balancing Statistics Reports

lab-422-g - Reports - Active Wireless Load Groups No refresh Refresh every secs

CNL-208-C20-1

Members	4
Clients	0
Average Load	0.0

AP	Radio	Load	State	Probes Declined	Auth/Assoc Declined	Rebalance Event
0500008043050356	1	0	Under-Loaded	0	0	0
0500008043050356	2	0	Under-Loaded	0	0	0
10490056235A0000	1	0	Under-Loaded	0	0	0
10490056235A0000	2	0	Under-Loaded	0	0	0

Members: 4 Clients: 0 Average Load: 0.0

In a client balancing/load control statistics report, the statistics reported for each client balancing load balance group are:

- **Members** — Number of radio members
- **Clients** — Total number of clients for all radio members
- **Average Load** — Average load for the group

The reported average load may not be correct in a failover situation. If some APs in the load balance group fail over the foreign controller, those APs will report to the foreign controller. The member APs will continue to use the member count for the whole group, but the member count displayed on the controller will be for only those APs that are reporting. Since the member count reported on the controller is not the complete set, the average will not be consistent with what the APs are using for the state determination.

The statistics reported for each member of the load balance group are:

- **AP** — AP name
- **Radio** — Radio number
- **Load** — Load value (number of clients currently associated with the AP)
- **State** — Load state
- **Probes Declined**
- **Auth/Assoc Requests Declined**
- **Rebalance Event** — Clients removed because of an over-loaded state

The report identifies SIAPP sub-groupings and provide separate group statistics for each sub-group.

When the load group includes sub-groups, **Average Load**, in red, is the average of the entire group. The average for each sub-group is also reported. The sub-group average is reported in red when group membership changes and not all members have been updated with the new member count.

Load balance group statistics are reported on the foreign controller when APs fail over with load groups from a different controller indicated with an "(F)" following the load group name.

Viewing Wireless AP Availability

In session availability, the **Wireless Availability** report displays the state of both the tunnels — active tunnel and backup tunnel — on both the primary and secondary wireless controllers.

The report uses a **Color Legend** to indicate the tunnel state:

- **Green** — AP has established an active tunnel.
- **Blue** — AP has established a backup tunnel.
- **Red** — AP is not connected.

In the report, each AP is represented by a box.

- The label, **Foreign** or **Local**, indicates whether the AP is local or foreign on the controller.
- The color in the upper pane of the box represents the state of the tunnel that is established to the current controller.



Note

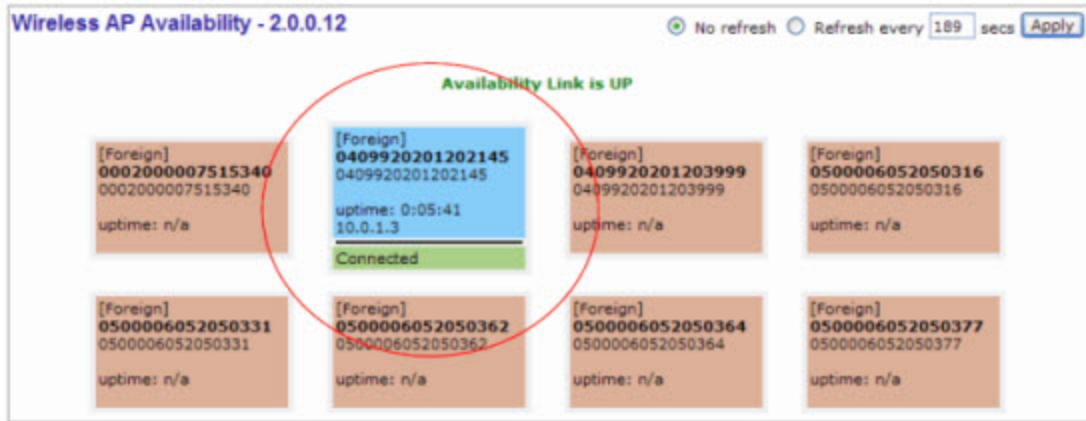
The current controller is the one on which the AP Availability report is viewed.

- The color in the lower pane of the box represents the state of the tunnel that is established with the other controller.

For the ease of understanding, take the example of the following scenario:

- Controller1 and Controller2 are paired in session availability
- A Wireless AP has established an active tunnel to Controller1.
- The same AP has established a backup tunnel to Controller2.

If you open the Wireless AP Availability report on Controller2, the report will appear as follows:



In the above example, the circled AP has established a backup tunnel to the foreign (secondary) controller, and an active tunnel to the local (Primary) controller.

AP Inventory Reports

To View Reports:

- 1 From the top menu, click **Reports**.
- 2 In the **Available AP** Reports list, click the report you want to view.



Note

All AP Inventory reports open in a new browser window.



Note

If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually time out.

The following is an example of the Wireless AP Inventory report:

lab13 - Reports - Wireless AP Inventory

Wireless AP (Serial)	Topology					HW			SW	Country	Antennas	Power Status	Sec. Tunnel	Cert.	SSH	
	Rdo	Admin	Ra	Rb	Rg	Rn	DP	BP	RT	FT	Req Ch	Ch / Tx	Aj	TxMn	TxMx	ATT
	11n Channel Width					11n Guard Interval					11n Protection Mo					
	Failure Maintn.					Assn			IP Address		Netmask		Gateway			
AP3825i_1404014508410000 (1404014508410000) Role:Traffic forwarder (AP) Location: /World/Thornh...	PHY_VLAN_103					Wireless AP3825i Internal			10.11.01.0196	Canada	-	N/A	-	-	-	SSH
	1	on	-	-							/				-	
	20MHz					-					None					
	2	on	-	-							/				-	
	20MHz					-					None					
enabled					DHCP			10.47.13.100		255.255.255.0		10.47.13.1				
AP3965i_1541D10030140001 (1541D10030140001) Role:Traffic forwarder (AP)	PHY_VLAN_103					Wireless AP3965i-ROW Internal			10.11.01.0196	Austria	-	Low PS:N/A Port1:AF Port2:N/A	-	-	-	SSH
	1	off	-	-							/				-	
	-					-					-					
	2	on	-	-							/				-	
	-					-					-					
disabled					DHCP			10.47.13.101		255.255.255.0		10.47.13.1				

Export

Table 119 lists the column names and abbreviations found in the AP Inventory report:

Table 119: AP Inventory Report Columns

Column Name	Description
Wireless AP (Serial)	Includes AP type, AP name, serial number, and role (including role type)
Topology	Ethernet port and associated IP address of the interface on the controller through which the AP communicates.
HW	Hardware version of the AP.
SW	Software version executing on the AP.
Country	Country in which the AP is deployed
Antennas	Antennas used
Power Status	Indicates ports on the AP39xx with low power status. Feature available for AP39xx only.
Sec. Tunnel	Secure tunnel mode
Cert.	AP certification (enabled or disabled)
SSH	SSH access (enabled or disabled)
LBS	Location-based service (enabled or disabled)
Mcast Assembly	Multicast Assembly (enabled or disabled)
BD	Broadcast disassociation (enabled or disabled).
Persistence	Enabled or disabled
P/To	Poll timeout. If polling is enabled, a numeric value.
P/I	Poll interval. If polling is enabled, a numeric value.

Table 119: AP Inventory Report Columns (continued)

Column Name	Description
Wired MAC	The physical address of the AP's wired Ethernet interface.
Description	As defined on the AP Properties screen.
Rdo	Radios: 1 or 2.
Ra	802.11a radio. The data entry for an AP indicates whether the a radio is on or off.
Rb	802.11b protocol enabled. Possible values are on or off.
Rg	802.11g protocol enabled. Possible values are on or off.
Rn	802.11n protocol enabled. Possible values are on or off.
DP	DTIM period
BP	Beacon Period
RT	RTS Threshold
FT	Fragmentation Threshold
Req Ch	Last requested channel
Ch / Tx	Current channel Tx power level
Aj	Auto Tx Power Ctrl Adjust when ATPC is enabled
TxMn	Minimum Tx power, in decibels
TxMx	Maximum Tx power, in decibels
ATT	Attenuation for APs that support professional antenna installation.
Dom	RF domain
MnBR	Minimum Basic Rate (For more information, see the Wireless AP radio configuration tabs.)
Pmb	Preamble (long, short)
PM	Protection Mode
PR	Protection Rate
PT	Protection Type
VNS Name: MAC	Also called BSSID, this is the MAC address of a (virtual) wireless interface on which the AP serves a BSS/VNS. There could be 8 per radio.
11n Channel Width	20MHz, 40MHz, or auto
11n Guard Interval	If 11n Channel Width is 40MHz, long or short
11n Channel Bonding	Enabled only if 11n Channel Width is 40MHz
11n Protection Mode	Protects high throughput transmissions on primary channels from non-11n APs and clients. Enabled or disabled.
Failure Maintn.	Maintain MU sessions on the Wireless AP when the AP loses the connection to the controller.
Assn	Assignment (address assignment method)

Table 119: AP Inventory Report Columns (continued)

Column Name	Description
IP Address	Wireless AP's IP address if statically configured (same as the Static Values button on the AP Static Configuration screen).
Netmask	If the AP's IP address is configured statically, the net mask that is statically configured for the AP.
Gateway	If the AP's IP address is configured statically, the IP address of the gateway router that the AP will use.
MTU Interface	MTU Interface (enabled or disabled)
MTU Tunnel	MTU Tunnel value
TLS	802.1x EAP-TLS authentication configuration
PEAP	802.1x PEAP authentication configuration
EWC Search List	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.



Channel Inspector Report

The Channel Inspector Report enhances Automatic Channel Selection (ACS) on the controller by providing an audit trail of selected channels and presenting a history of channel selection. The channel data generated from ACS populates the report, or you can initiate a channel scan on-demand from the user interface. The report is generated from the last channel scan. The date and time of the last channel scan appear on the report.

Related Links

[Viewing the Channel Inspector Report](#) on page 582

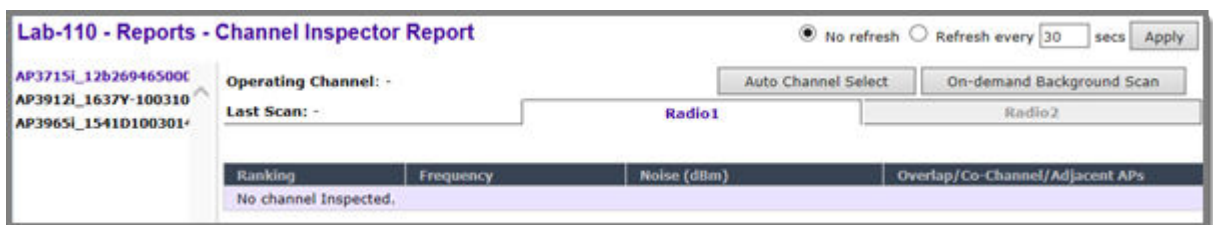
[Running a Background Scan](#) on page 583

[Channel Inspector Report Fields](#) on page 583

Viewing the Channel Inspector Report

To view the Channel Inspector Report:

- 1 From the top menu, click **Reports**.
- 2 Select **Channel Inspector**.



Running a Background Scan

Background scan extends the usefulness of the Automatic Channel Scan (ACS) feature. It is a reporting tool that helps you verify and understand channel assignments. Where ACS is a disruptive and persistent channel assignment, the on-demand background scan runs without disrupting service. To verify channel assignments and review channel details without having to run a full ACS, run an on-demand background scan.

The background scan does not change channel assignments, it simply provides details about the current assignments. Run background scan on each radio separately. To change channel assignments, you must run ACS.

From the Channel Inspector Report, click **On-Demand Background Scan**.

Related Links

[Channel Inspector Report Fields](#) on page 583



Channel Inspector Report Fields

Table 120: Channel Inspector Report

Field	Description
Operating Channel	Indicates the operating channel of the AP. This is not necessarily the highest ranked channel. For best performance, you want the highest ranked channel to be the operating channel.
Last Scan	Date and time of the last background scan.
Refresh	Auto refresh ensures that the most recent scan data is presented. Enable or disable auto refresh at the top of the report. 30 seconds is the default auto refresh value. If auto refresh is disabled, click the Refresh button to manually refresh the display.
Auto Channel Select	Initiates Auto Channel Selection (ACS). ACS is a disruptive and persistent channel assignment. Use this option to reassign the channels. The ACS scan will disrupt network activity.
On-Demand Background Scan	The background scan does not change channel assignments, it simply provides details about the current assignments. Run background scan on each radio separately. To change channel assignments, you must run ACS.
Ranking	Indicates the best operating channel based on a 5-star ranking. This ranking is relative to the channels that are available.
Frequency	Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
Noise	Channel noise measured in Decibel-milliwatts (dBm).

Table 120: Channel Inspector Report (continued)

Field	Description
Channel Details Interference Type	Click the details link to display the following channel details: Describes the channel interference in relation to the operating channel. Possible values are: <ul style="list-style-type: none"> • Co-Channel. All the APs on the same channel as the target AP are competing. Using Distributed Control Function (DCF) collisions are avoided because the APs know to avoid each other; however, the more traffic on the channel the greater the chance of collisions. Throughput slows but all packets get through. • Adjacent. APs on adjacent channels are close enough to interfere, but not close enough to know they are interfering. They do not have the benefit of DCF. • Overlapping. Applicable for 40MGz and 80MGz channels only. The 20MGz channel is designated as the primary and the other channels are designated as extension channels (secondary). If the primary channel of one AP is the same as the extension channel of another AP it is considered overlapping. Overlapping is the worst type of interference. Example Notation, Co-Channel 20 44: (5220) indicates that there is co-channel interference on the beacon channel 5220.
Frequency	Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
RSS	Received signal strength value.
BSSID	Basic Service Set Identifier. Identifies the AP.
SSID	Service Set Identifier. Identifies the network.
AP Name	Name of the AP provided at network setup.

AP Performance by Radio Report

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

- Click the **AP Performance by Radio** display option. The **AP Performance by Radio** display opens in a new browser window.

lab13 - Reports - AP Performance Report by Radio No refresh Refresh every 30 secs Apply

Wireless AP	Radio Mode	Chd Util (%)				RSSI (dBm)				SNR (dB)				Packet Retransmissions (pps)			
		Peak		Avg		Peak		Avg		Peak		Avg		Peak		Avg	
		Prev	Cur	Cur	Cur	Prev	Cur	Cur	Cur	Prev	Cur	Cur	Cur	Prev	Cur	Cur	Cur
AP3715_12b2694650000003	a/n	0	0	0	0	0	0	-18	-3	0	94	78	92	0	2	0	0
AP3715_12b2694650000003	b/g	0	0	0	0	0	0	-85	N/A	0	95	10	-5	0	5	0	0

Data as of Mar 16, 2015 10:08:32 am Refresh Export Close

AP Performance by SSID and Radio Report

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

- Click the **AP Performance by SSID and Radio** display option. The **AP Performance by SSID and Radio** display opens in a new browser window.

LAB62 - Reports - AP Performance Report by SSID and Radio No refresh Refresh every 30 secs Apply

Wireless AP	Radio Mode	SSID	# of Clients				Uplink Throughput								Downlink Throughput							
							Bytes Per Second				Packets Per Second				Bytes Per Second				Packets Per Second			
			Peak	Avg	Cur	Cur	Peak	Avg	Cur	Cur	Peak	Avg	Cur	Cur	Peak	Avg	Cur	Cur	Peak	Avg	Cur	Cur
13310613085D0000	a	LAB6162	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13310613085D0000	a	ACTT	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13310613085D0000	b/g	LAB6162	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Data as of Mar 16, 2015 10:20:31 am Refresh Export Close

AP Accessibility Report

- From the top menu, click **Reports**. The **Available AP Reports** screen displays.

- Click the **AP Accessibility Report** display option. The **AP Accessibility Report** display opens in a new browser window.

lab13 - Reports - AP Accessibility Report No refresh Refresh every 30 secs

Wireless AP	Radio Mode	Assoc. Req. Rx				Reassoc. Req. Rx				Deassoc./Disauth Req. Tx				Deassoc./Disauth Req. Rx						
		Peak		Avg	Cor	Peak		Avg	Cor	Peak		Avg	Cor	Peak		Avg	Cor			
		Prev	Cur			Prev	Cur			Prev	Cur			Prev	Cur					
AP3715_12b2694650000000	a/n	0	8	2	0	0	0	0	0	0	0	0	0	2	0	0	0	2	2	0
AP3715_12b2694650000000	b/g	0	12	0	5	0	3	0	0	0	0	5	0	1	0	0	0	0	0	0

Data as of Mar 16, 2015 10:07:16 am



Viewing All Clients

View a list of all clients and take action on one or more clients in the list. You can also export the list of clients to an XML file.

- 1 From the top menu, click **Reports > Clients**.

Client IP	Device Type	AP	WLAN	Time Seen	RSS	Role
<input type="checkbox"/> 172.29.163.114	Unknown	CS110 - ap3 - AP3825e	CNL-218-3-14-ssid	12:24:19	-22	CNL-218-14-default

Showing 1 to 1 of 1 entries
 L:LDPC; S:STBC; T:TxBF; M:MU_MIMO; F:FT; W:PMF

Buttons: Add to Blacklist, Disassociate, Show OUI, Export

Figure 159: All Client Report

- 2 Use the Search facility to find a specific client. For more information, see [Client Search Facility](#) on page 590.



Note

Clients supporting 802.11W Protected Management Frame (PMF) display a W in the client Protocol field.

- 3 To take action on one or more clients, select the checkbox for the client and click one of the action buttons:
 - **Add to Blacklist.** Add the selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the AP.
 - **Disassociate.** Cut the connection with a particular wireless device.
 - **Show OUI.** The Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies the client vendor or manufacturer.
 - **Export.** Export selected clients to an XML file. System prompts you to open or save the XML file.
- 4 To view client details, click the client row (not the checkbox). For more information, see [Displaying Client Details](#) on page 588.



Displaying Client Details

Display client details to determine client activity and usage of network resources. From the All Client report, you can display the following information for each client:

- 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.

- 1 Go to **Reports** > **Clients**.

The All Clients report appears.

- Click on a client row (not the checkbox).

The **Detailed Information** dialog for the client appears.

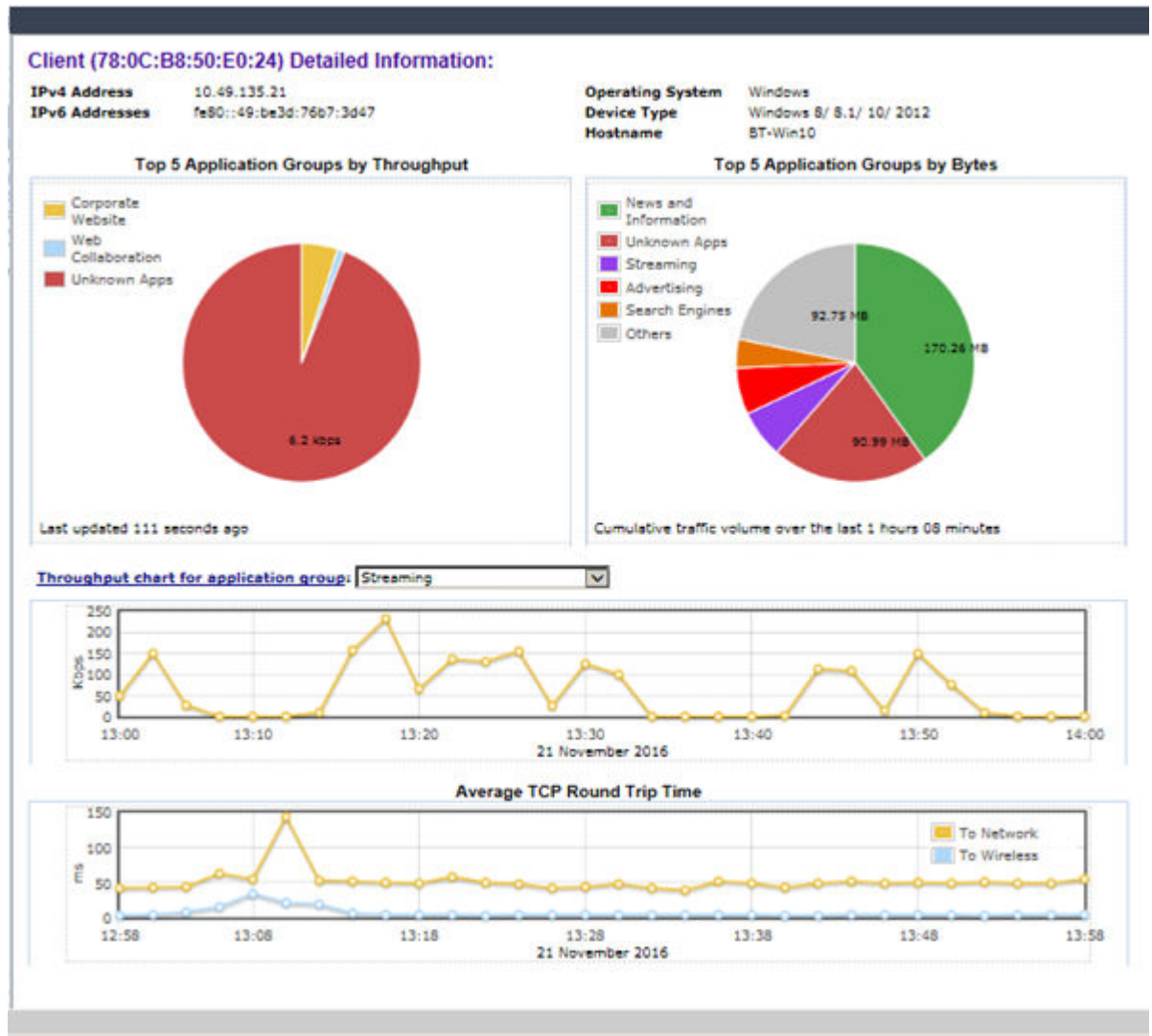


Figure 160: Client Detailed Information

Related Links

[Application Visibility and Device ID](#) on page 566




Client Search Facility

Search for any part of the client string.

Results:

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

To search, do the following:

- 1 Go to **Reports > Clients**.
- 2 At the top of the screen, enter search criteria and click . Clients that match the search criteria are displayed in the list.

Lab-110 - Reports - Active Clients Report

x
🔍
↻

<input type="checkbox"/>	Client IP	Device Type	AP	WLAN	Time Seen
<input type="checkbox"/>	172.16.209.8	Unknown	AP3715i_12b 2694650000 000	Lab126-110- AAAMF5	11:06:03

Showing 1 to 1 of 1 entries

Figure 161: All Clients Search



Viewing Client MAC and OUI

Take the following steps to view the MAC address and OUI for selected clients. The Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies the client vendor or manufacturer.

- 1 From the top menu, click **Reports > Clients**.
- 2 Select the checkbox next to a client row and click **Show OUI**.

The Client MAC and OUI Full Name for the selected client display.

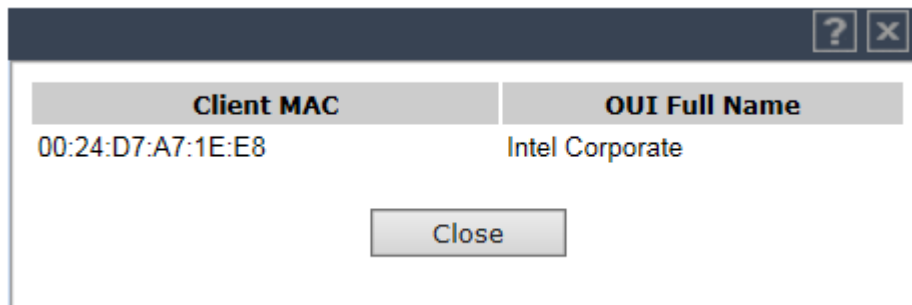


Figure 162: Show OUI dialog

Viewing Role Filter Statistics

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

- 2 In the left pane, click **Filter Statistics**. The **Available Filter Statistics Reports** screen displays.

The screenshot shows a web interface with a top navigation bar containing 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. A 'Logout' link is visible in the top right. The left sidebar has a menu with 'APs', 'Clients', 'Filter Statistics' (highlighted), 'Role Filter Statistics', 'Topology Filter Statistics', 'Topology', 'Mobility', 'Radar', 'Controller Status', 'Routing Protocols', and 'RADIUS'. The main content area is titled 'Available Filter Statistics Reports' and contains two buttons: 'Role Filter Statistics' and 'Topology Filter Statistics'.

- 3 Under Available Filter Statistics Reports, click **Role Filter Statistics**. The **Role Filter Statistics** display opens in a new browser window.

lab-422-g - Reports - Role Filter Statistics No refresh Refresh every 30 secs

Role	Packets Allowed	Packets Denied
CNL-422-0-0-default	0	0
CNL-422-0-0-non-authenticated	0	0
CNL-422-0-1-default	0	0
CNL-422-0-1-non-authenticated	0	0
CNL-422-0-2-default	0	0
CNL-422-0-2-non-authenticated	0	0
CNL-422-0-3-default	0	0
CNL-422-1-2-wds-default	0	0
CNL-422-1-2-wds-non-authenticated	0	0
CNL-422-1-4-wds-default	0	0
CNL-422-1-5-default	0	0
CNL-422-1-5-non-authenticated	0	0
CNL-422-1-6-default	0	0
CNL-422-1-7-default	0	0
CNL-422-1-7-non-authenticated	0	0
CNL-422-2-10-default	0	0
CNL-422-2-11-default	0	0
CNL-422-2-11-non-authenticated	0	0
CNL-422-2-12-wds-default	17867	0
CNL-422-2-8-default	0	0
CNL-422-2-9-default	0	0
CNL-422-3-12-default	0	0
CNL-422-3-13-default	0	0
CNL-422-3-14-default	0	0
CNL-422-3-15-wds-default	0	0

Total Invalid Role Count: 3011515936

Data as of Mar 03, 2014 11:29:56 am

- Statistics are expressed in respect to the AP. Therefore, Packets Allowed indicates the packets the AP has received from a client and Packets Denied indicates the packets the AP has rejected.
- A client is displayed as soon as the client connects (or after a refresh of the screen). The client disappears as soon as it times out.

- 4 Under Available Filter Statistics Reports, click **Topology Filter Statistics**. The **Topology Filter Statistics** display opens in a new browser window.

lab-422-g - Reports - Topology Filter Statistics No refresh Refresh every secs

Topology	Packets Allowed	Packets Denied
Port1	17831	0
Port2	3060	0
Port3	0	0
Port4	0	0
CNL-422-0-0	0	0
CNL-422-0-1	0	0
CNL-422-0-2	0	0
CNL-422-0-3	0	0
CNL-422-1-5	0	0
CNL-422-1-6	0	0
CNL-422-1-7	0	0
CNL-422-2-10	0	0
CNL-422-2-11	0	0
CNL-422-2-12-wds	2	2146
CNL-422-2-9	0	0
CNL-422-3-12	0	0
CNL-422-3-13	0	0
CNL-422-3-14	0	0
CNL-422-3-15-wds	0	0

Data as of Mar 03, 2014 11:31:36 am

- Statistics are expressed in respect to the AP. Therefore, Packets Allowed indicates the packets the AP has received from a client and Packets Denied indicates the packets the AP has rejected.
- A client is displayed as soon as the client connects (or after a refresh of the screen). The client disappears as soon as it times out.

Viewing Topology Reports

Topology Statistics — Displays statistics for total sent and received packets, octets, multicast packets, and broadcast packets.

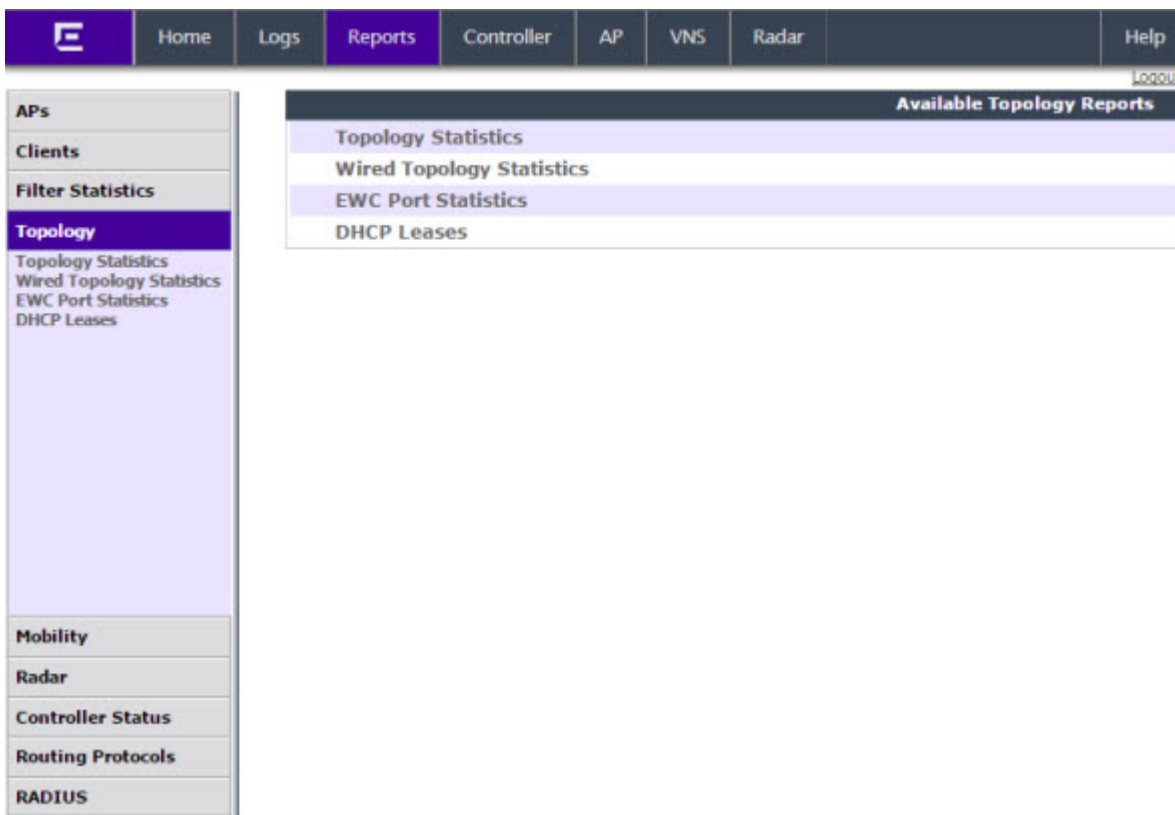
Wired Topology Statistics — Displays statistics for each topology including total packets sent and received.

EWC Port Statistics — Displays port statistics for active Topologies including current status and totals for frames, octets, multicast frames and broadcast frames sent and received.

DHCP Leases — Displays statistics to help determine if you have sufficient addresses for your needs and whether the lease times are too long.

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

- In the left pane, click **Topology**. The **Available Topology Reports** screen displays.



- Under Available Topology Reports, click **Topology Statistics**. The **Topology Statistics** display opens in a new browser window.

lab-422-g - Reports - Topology Statistics No refresh Refresh every 30 secs

Topology	Packets		Octets		Multicast Packets		Broadcast Packets	
	Sent	Received	Sent	Received	Sent	Received	Sent	Received
Port1	71684	77969	13818710	14510451	2787	9014	3104	3104
Port2	6447	8542	2901376	3062392	158	2276	3096	3096
Port3	1	0	60	0	0	0	0	0
Port4	0	0	0	0	0	0	0	0
CHL-422-0-0	0	0	0	0	0	0	0	0
CHL-422-0-1	0	0	0	0	0	0	0	0
CHL-422-0-2	202	2298	9924	171000	158	2276	0	0
CHL-422-0-3	0	0	0	0	0	0	0	0
CHL-422-1-5	0	0	0	0	0	0	0	0
CHL-422-1-6	0	0	0	0	0	0	0	0
CHL-422-1-7	0	0	0	0	0	0	0	0
CHL-422-2-9	0	0	0	0	0	0	0	0
CHL-422-2-10	200	2297	9804	170940	158	2276	0	0
CHL-422-2-11	0	0	0	0	0	0	0	0
CHL-422-2-12-wds	14179	21550	1211132	2620320	0	6116	4337	2169
CHL-422-3-12	0	0	0	0	0	0	0	0
CHL-422-3-13	0	0	0	0	0	0	0	0
CHL-422-3-14	0	0	0	0	0	0	0	0
CHL-422-3-15-wds	0	0	0	0	0	0	0	0

Data as of Mar 03, 2014 11:35:17 am

- 4 Under Available Topology Reports, click **Wired Topology Statistics**. The **Wired Topology Statistics** display opens in a new browser window.

EWC - Reports - Wired Topology Statistics No refresh Refresh every secs

Topology ▾	Group ⇅	Total Packets		Octets		Multicast Packets		Broadcast Packets	
		Sent ⇅	Received ⇅	Sent ⇅	Received ⇅	Sent ⇅	Received ⇅	Sent ⇅	Received ⇅
physical 1	No	6854	6856	4042788	4042908	2	2	6852	6852

Data as of May 22, 2015 09:13:18 am

- 5 Under Available Topology Reports, click **EWC Port Statistics**. The **EWC Port Statistics** display opens in a new browser window.

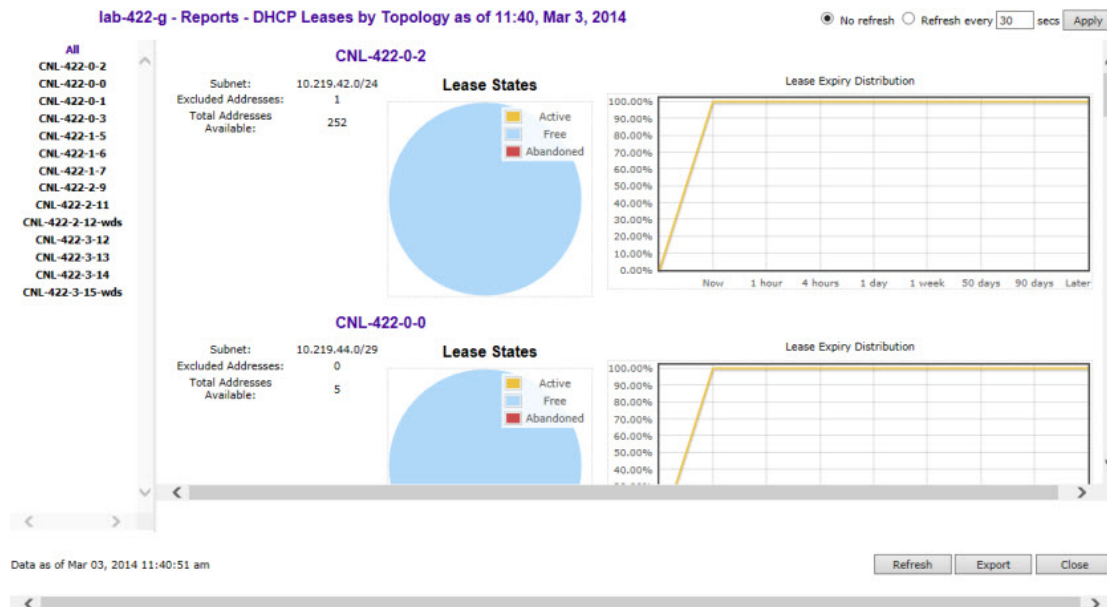
lab-422-g - Reports - Wireless Controller Port Statistics No refresh Refresh every secs

Port Statistic	Port1	Port2	Port3	Port4	lag1	lag2
Current Status	UP	UP	DOWN	DOWN	DOWN	DOWN
Frames Sent	32404	3666	0	0	0	0
Frames Received	57525	111983	0	0	0	0
Octets Sent	5162655	1881552	0	0	0	0
Octets Received	11167393	15755957	0	0	0	0
Multicast Frames Sent	2814	480	0	0	0	0
Multicast Frames Received	17663	48625	0	0	0	0
Broadcast Frames Sent	3123	3120	0	0	0	0
Broadcast Frames Received	99	59736	0	0	0	0

Data as of Mar 03, 2014 11:38:06 am

- Statistics are expressed in respect to the AP. Therefore, **Frames Sent** indicates packets sent to the AP from a client and **Frames Received** indicates the packets received from the AP.

- 6 Under Available Topology Reports, click **DHCP Leases**. The **DHCP Leases** display opens in a new browser window.



The report applies only to the DHCP server hosted on the local controller. The report is empty if DHCP is not enabled on any of the controller's topologies. Otherwise, for each of the controller's topologies the report provides a summary table of the address range, number of excluded address and total addresses available, a pie chart showing the proportion of addresses that are free, in use or abandoned, and a graph that shows how many leases will become available at different times assuming that no more leases are handed out by the server from this instant.

Abandoned leases should rarely be seen. The presence of one or more abandoned leases indicates that another DHCP server may be operating on the same subnet, resulting in IP address conflicts. The server abandons the use of any address it thinks is being managed by another DHCP server.

The lease expiry graph indicates the proportion of available leases that will be available now, 1, 4 hours, 1 day, 1 week 50 and 90 days from now assuming that the server never hands out another lease. If the network serves a relatively small number of users, who are in fact the same users day in and day out, then you should use longer lease times, meaning that this graph should not show 100% address availability until farther to the right in the graph. If you have a high turn over of users (like in a university classroom that has a different set of people every 1 hour) then you should use shorter lease times (achieve 100% availability more towards the left in the graph). If you find that you are running out of addresses, you should use the line graph to decide if you can afford to shorten lease times to make leases available sooner as opposed to creating a new, bigger subnet to handle more users concurrently.

Viewing Mobility Reports

The Mobility Domain is a virtual combination of Wireless LAN Controllers (WLCs) grouped for the purpose of roaming. The controller group consists of a Mobility Manager, Mobility agents, and a Backup Mobility Manager. The Mobility Domain preserves information about user sessions, allowing users to roam through the use of identity-based networking. A Mobility Domain can also provide network flexibility and scalability.

When a controller has been configured as a mobility manager, additional displays appear as options in the left pane:

- **Primary Manager Mobility Tunnel Matrix** — Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain.
- **Client Location in Mobility Zone** — Displays the active wireless clients and their status.
- **Backup Manager Mobility Tunnel Matrix** — Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain.
- **Remotable VNS** — Displays the active wireless clients and their status.



Note

There are four possible reports available from the **Available Mobility Reports** page depending on the configuration of the controller. If the controller does not have mobility enabled, it will just include the **Remotable VNS** report.

To view Mobility Manager reports:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Mobility**.
- 3 Click the appropriate mobility manager report:
 - Client Location in Mobility Zone
 - Backup Manager Mobility Tunnel Matrix
 - Remotable VNS
 - Primary Manager Mobility Tunnel Matrix

The colored status indicates the following:

- **Green** — The mobility manager is in communication with an agent and the data tunnel has been successfully established.
- **Yellow** — The mobility manager is in communication with an agent but the data tunnel is not yet successfully established.
- **Red** — The mobility manager is not in communication with an agent and there is no data tunnel.

Client Location in Mobility Zone

This report displays the active wireless clients and their status.

EWC	Client IP	Client MAC Address	User	Current EWC
C4110-NAM (10.100.1.1) 0 mobility clients				
No clients connected with home EWC 10.100.1.1				
tunnels:	10.100.3.1		10.200.1.1	
C5110-ROW (10.100.3.1) 0 mobility clients				
No clients connected with home EWC 10.100.3.1				
tunnels:	10.100.1.1		10.200.1.1	
C25-ROW (10.200.1.1) 2 mobility clients				
	10.200.2.56	00:1C:10:2A:FB:0C	N/A	10.200.1.1
	10.200.2.245	00:1F:3B:21:57:53	N/A	10.200.1.1
tunnels:	10.100.1.1		10.100.3.1	

Data as of Mar 17, 2014 01:03:38 pm

Refresh Export Close

Figure 163: Client Location in Mobility Zone Report

You can do the following:

- Sort this display by home or foreign controller.
- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box.
- Define the refresh rates for this display.
- Export this information as a .xml file.

Primary/Backup Manager Mobility Tunnel Matrix

This report displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain.

The following report illustrates a mobility setup with three controllers:

- Mobility Manager (M) (10.105.0.5)
- Mobility Agent/Backup Manager (BM) 10.105.0.9
- Mobility Agent (10.105.0.7)

In the following illustration, there is one client on the Primary Manager (M) and 0 clients on the other controllers. As the client moves through the Mobility group, the number of clients will change from 0 to 1 depending on which tunnel the client moves through. This report graphically displays the number of data tunnels, number of active mobility clients, and the number of clients on each controller.

Downed tunnels are represented in brown. **No tunnels: 0** indicates that all tunnels are up.

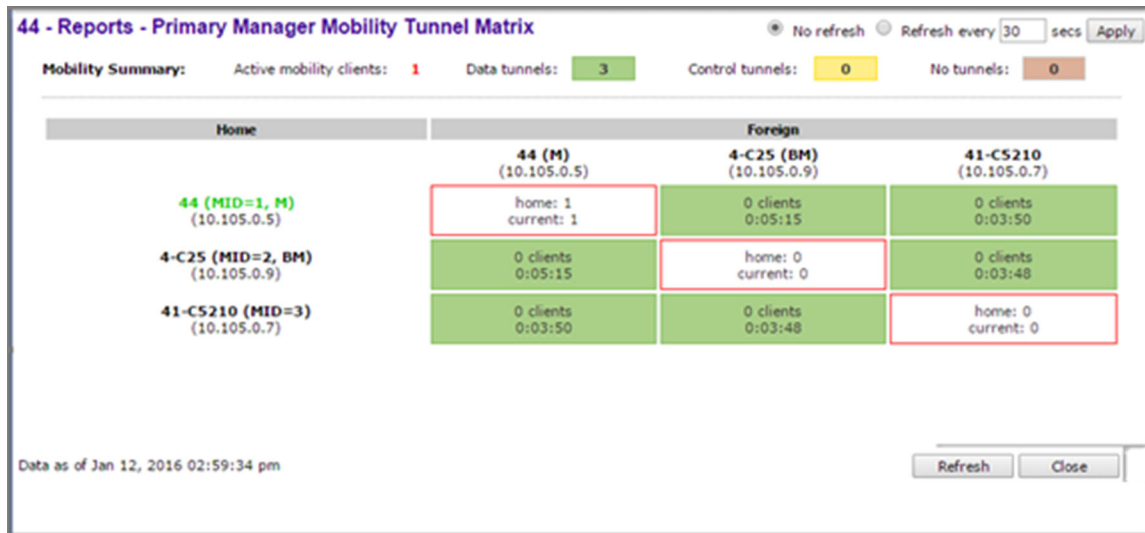


Figure 164: Primary/Backup Manager Mobility Tunnel Matrix

This report provides the following information:

- Provides connectivity matrix of mobility state.
- Provides a view of:
 - Tunnel state
 - If a tunnel between controllers is reported down, it is highlighted in red.
 - If only a control tunnel is present, it is highlighted in yellow.
 - If data and control tunnels are fully established, it is highlighted in green.
 - Tunnel Uptime
 - Number of clients roamed (Mobility loading)
 - Local controller loading
 - Mobility membership list

A controller is only removed from the mobility matrix if an administrator explicitly removes it from the by Mobility permission list. If there is a link between controllers, or the controller is down, the corresponding matrix connections are identified in red to identify the link.

The Active Clients by VNS report for the controller on which the user is home (home controller) will display the known user characteristics (IP, statistics, etc.). On the foreign controller, the Clients by VNS report does not show users that have roamed from other controllers, since the users remain associated with the home controller's VNS.

The Active Clients by AP report on each controller will show both the loading of local and foreign users (users roamed from other controllers) that are taking resources on the AP.



Note

Although you can set the screen refresh period less than 30 seconds, the screen will not be refreshed quicker than 30 seconds. The screen will be refreshed according to the value you set only if you set the value above 30 seconds.

Remotable VNS

This report displays the active wireless clients and their status.

SSID ▲	Privacy ◆	Home Controller ◆
CNL1050-1S-4wep	None	44
CNL1050-1S-4wep	None	4-C25

Figure 165: Remotable VNS Report

You can do the following:

- Sort this display by home or foreign controller.
- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box.
- Define the refresh rates for this display.
- Export this information as an xml file.

Viewing Controller Status Information

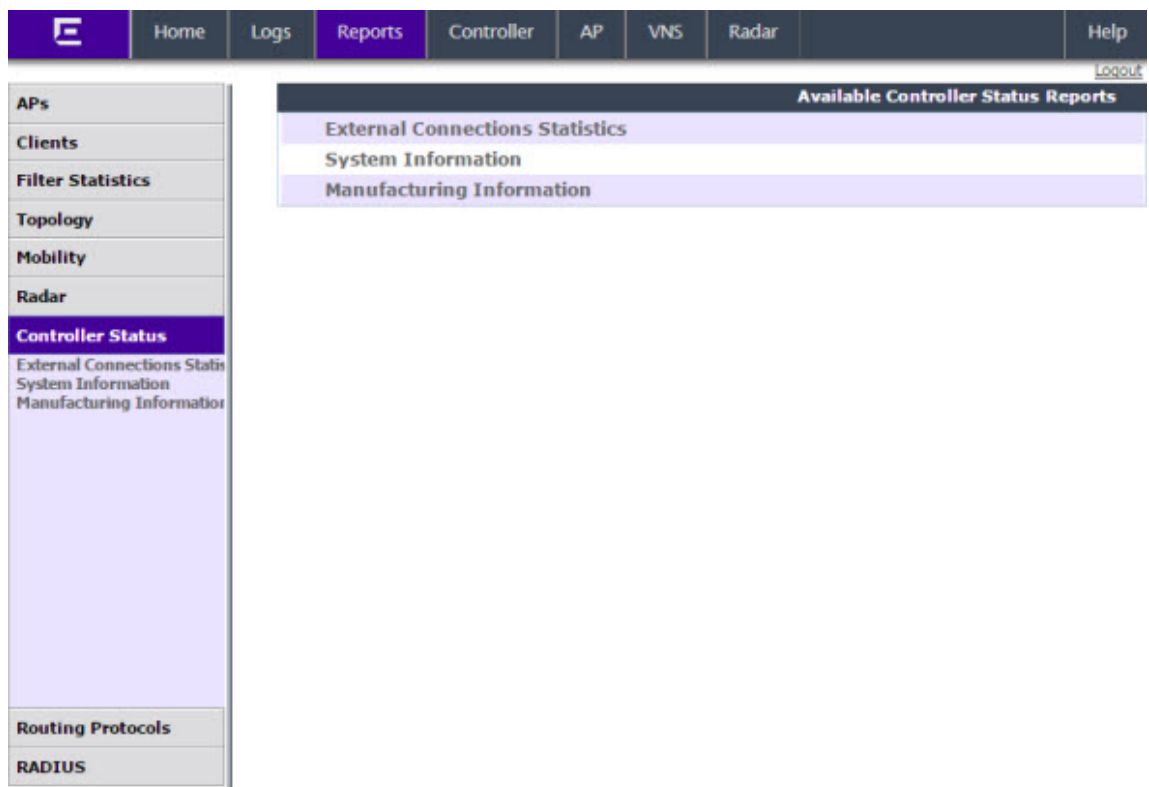
External Connection Statistics— Displays connection information including security level.

System Information — Displays system information including memory usage and CPU and board temperatures.

Manufacturing Information — Displays manufacturing information including the card serial number and CPU type and frequency.

To View External Connection Statistics:

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Controller Status**. The **Available Controller Status Reports** screen displays.



- 3 Click the **External Connection Statistics** option. The **External Connection Statistics** display opens in a new browser window.

lab-422-g - Reports - External Connections Statistics No refresh Refresh every secs

Total: 0

Connection	Security Level
No external connections found.	

Data as of Mar 03, 2014 11:48:52 am

To View System Information:

- 4 From the top menu, click **Reports**.
- 5 In the left pane, click **Controller Status**. The **Available Controller Status Reports** screen displays.

- 6 Click the **System Information** display option. The **System Information** display opens in a new browser window.

lab-422-g - Reports - System Information No refresh Refresh every secs

```

System Information
System Up Time: 5:45
- CPU Utilization: 7.60
- Memory Usage:
  Free: 80 %
- Disk Usage (1 Kbyte blocks)
  Partition    Total Space    Used    Available    Use %
  root         27193624      430032    25944520     2%
  tmp          131072        356      130716       1%
  home         2040016      32840    1986696      2%
  cdr          2032048      32824    1978744      2%
  logs         1528032      33316    1479376      3%
  reports      1522032      32812    1473880      3%
  trace        1531008      32812    1482866      3%
- System Temperature
  Processor 1 Temperature: -61 C degrees below meltdown
  Power Supply 1 Temperature: 33 C
  Power Supply 2 Temperature: 34 C
  Memory Module 1 Temperature: 29 C
  System Board 1 Ambient Temperature: 22 C
  System Board 1 Planar Temperature: 31 C
- Fan Speed
  1A Fan: 5640 RPM
  1B Fan: 3960 RPM
  2A Fan: 6640 RPM
  2B Fan: 3960 RPM
  3A Fan: 4920 RPM
  3B Fan: 3480 RPM
  4A Fan: 4920 RPM
  4B Fan: 3480 RPM
  5A Fan: 5040 RPM
  5B Fan: 3480 RPM
- Port1 Interface:
  Auto-negotiation: enabled
  Auto-negotiation capability includes:
    any speed and any duplex
  Interface State: up, 1000Mbps full duplex
- Port2 Interface:
  Auto-negotiation: enabled
  Auto-negotiation capability includes:
    any speed and any duplex
  Interface State: up, 1000Mbps full duplex
- Port3 Interface:
  Auto-negotiation: enabled
  Auto-negotiation capability includes:
    any speed and any duplex
  Interface State: down
- Port4 Interface:
  Auto-negotiation: enabled
  Auto-negotiation capability includes:
    any speed and any duplex
  Interface State: down

```

Data as of Mar 03, 2014 11:51:10 am

To View Manufacturing Information:

- 7 From the top menu, click **Reports**.
- 8 In the left pane, click **Controller Status**. The **Available Controller Status Reports** screen displays.

- Click the **Manufacturing Information** display option. The **Manufacturing Information** display opens in a new browser window.

WLC - Reports - Manufacturing Information

Manufacturing Information

```
Manufacturing ID (Serial Number): B4858436
BIOS Version: V12.01.03
Hardware Revision: ES003
Software Version: 08.31.01.1022D
Model: WLC711
CPU Type: Intel(R) Core(TM)2 Duo CPU      U9300  @ 1.20GHz
CPU Frequency (MHz): 1197.129
HW Encryption Support: No
LAN   MAC address: 00:0E:8C:EB:CD:CD
ADMIN MAC address: 00:0E:8C:EB:CD:BA
```

Viewing Routing Protocol Reports

The following reports are available in the Extreme Networks ExtremeWireless system:

- **Forwarding Table** — Displays the defined routes, whether static or OSPF, and their current status.
- **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.

To View the Forwarding Table:

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

- In the left pane, click **Routing Protocols**. The **Available Routing Protocols Reports** screen displays.

The screenshot shows a web interface with a navigation menu at the top and a left sidebar. The navigation menu includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The Reports menu is currently selected. The left sidebar contains a list of menu items: APs, Clients, Filter Statistics, Topology, Mobility, Radar, Controller Status, Routing Protocols (highlighted), Forwarding Table, OSPF Neighbor, OSPF Linkstate, and RADIUS. The main content area displays the 'Available Routing Protocols Reports' screen, which lists three report types: Forwarding Table, OSPF Neighbor, and OSPF Linkstate.

Available Routing Protocols Reports	
Forwarding Table	
OSPF Neighbor	
OSPF Linkstate	

- 3 Click the **Forwarding Table** option. The **Forwarding Table** displays in a new browser window.

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



Note

If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually time out.

To view the OSPF Neighbor Table:

- 4 From the top menu, click **Reports**.
- 5 In the left pane, click **Routing Protocols**.

- 6 Click the **OSPF Neighbor** option. The **OSPF Neighbor** displays in a new browser window.

lab-422-g - Reports - OSPF Neighbor No refresh Refresh every 30 secs

Neighbor Router ID	Router Priority	State	IP Address	Interface Name
192.168.14.1	1	Full/DR	10.219.40.2	Port1:10.219.40.1

Data as of Mar 03, 2014 11:56:12 am

To View the OSPF Linkstate Table:

- 7 From the top menu, click **Reports**. The **Available AP Reports** screen displays.
- 8 In the left pane, click **Routing Protocols**.
- 9 Click the **OSPF Linkstate** option. The **OSPF Linkstate** displays in a new browser window.

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

Router LSA (Type 1)

Link ID	Advertising Router	Age	Sequence Number	checkSum	Link Count
192.168.3.92	192.168.3.92	331	0x800010c7	0x6efc	2
192.168.3.110	192.168.3.110	5	0x80000016	0x8ec9	14
192.168.3.116	192.168.3.116	64	0x800019d1	0x7f4d	6
192.168.3.182	192.168.3.182	1570	0x80007cdd	0x29d9	4
192.168.3.200	192.168.3.200	405	0x80001e1d	0x16be	4
192.168.3.219	192.168.3.219	1192	0x800000b7	0x4ca2	6
192.168.3.225	192.168.3.225	6	0x80000094	0xb7f9	4
192.168.14.1	192.168.14.1	38	0x80008747	0xc868	176
192.168.14.4	192.168.14.4	1747	0x80000096	0xb890	4
192.168.14.11	192.168.14.11	119	0x80000016	0x2112	14
192.168.14.15	192.168.14.15	282	0x80000015	0x78f3	14
192.168.14.16	192.168.14.16	118	0x8000000c	0x8049	14
192.168.14.47	192.168.14.47	1462	0x8000039d	0x3770	2
192.168.14.48	192.168.14.48	570	0x8000021a	0xed2a	2
192.168.14.49	192.168.14.49	310	0x80000007	0xc960	3
192.168.14.50	192.168.14.50	61	0x800001e1	0x5b22	3
192.168.14.181	192.168.14.181	780	0x80000098	0x6184	4
192.168.14.182	192.168.14.182	1549	0x800000c0	0x1c10	3

Network LSA (Type 2)

Link ID	Advertising Router	Age	Sequence Number	checkSum
10.11.0.2	192.168.14.1	351	0x80001dfe	0xf40c
10.12.0.2	192.168.14.1	351	0x80001dfe	0xe817
10.51.0.2	192.168.14.1	771	0x800001dc	0xfea3
10.52.0.2	192.168.14.1	291	0x80000004	0x99e2

Data as of Mar 03, 2014 12:07:22 pm

To Export and Save a Report in XML:

- 10 On the report screen, click **Export**. A Windows **File Download** dialog is displayed.
- 11 Click **Save**. A Windows **Save As** dialog is displayed.



Note

If your default XML viewer is Internet Explorer or Netscape, clicking Open will open the exported data to your display screen. You must right-click to go back to the export display. The XML data file will not be saved to your local drive.

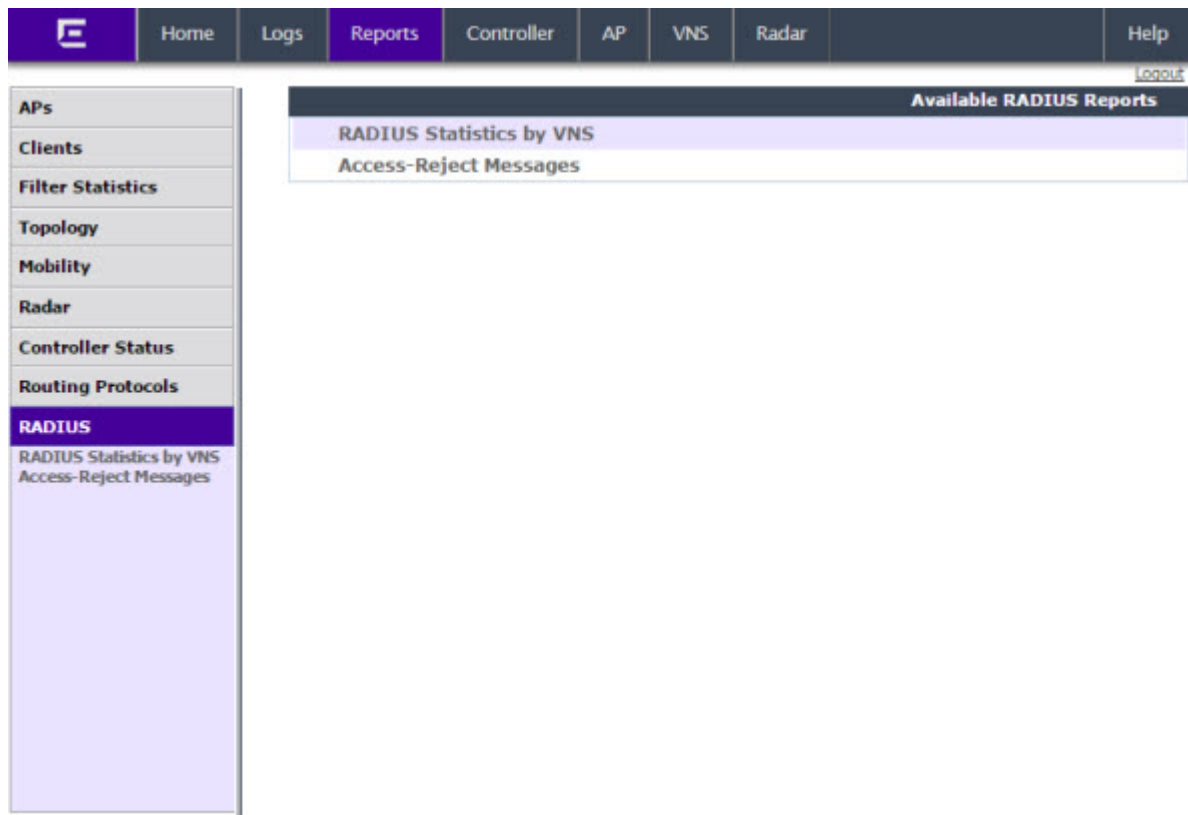
- 12 Browse to the location where you want to save the exported XML data file, and in the **File name** box enter an appropriate name for the file.
- 13 Click **Save**. The XML data file is saved in the specified location.

Viewing RADIUS Reports

The following RADIUS reports are available in the Extreme Networks ExtremeWireless system:

- **RADIUS Statistics by VNS** — Displays a list of VNS along with the number of Requests and their status (Failed or Rejected).
- **Access-Reject Reply-Message** — Displays the current list of messages along with an active count of all messages.

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **RADIUS**. The **Available RADIUS Reports** screen displays.



- 3 Click **RADIUS Statistics by VNS** option. The report displays in a new browser window.

lab-422-g - Reports - RADIUS Statistics by VNS No refresh Refresh every 30 secs

VNS	Requests	Failed	Rejected
CNL-422-0-0	0	0	0
CNL-422-0-1	0	0	0
CNL-422-0-2	0	0	0
CNL-422-0-3	0	0	0
CNL-422-1-2-wds	0	0	0
CNL-422-1-4-wds	0	0	0
CNL-422-1-5	0	0	0
CNL-422-1-6	0	0	0
CNL-422-1-7	0	0	0
CNL-422-2-10	0	0	0
CNL-422-2-11	0	0	0
CNL-422-2-12-wds	25	0	0
CNL-422-2-8	0	0	0
CNL-422-2-9	0	0	0
CNL-422-3-12	0	0	0
CNL-422-3-13	0	0	0
CNL-422-3-14	0	0	0
CNL-422-3-15-wds	0	0	0
CNL-422-WDS	0	0	0

Data as of Mar 03, 2014 11:36:58 am

- 4 To View the Access-Reject Messages, in the left pane, click **Access-Reject Messages** option.

lab13 - Reports - Access-Reject Messages No refresh Refresh every 30 secs

Access-Reject Reply-Message	Count
Controller - No Response from RADIUS Server.	4
Controller - No RADIUS Server Available.	1

Data as of Feb 27, 2015 03:28:05 pm

- 5 Click **Save**. A **Save As** dialog is displayed.

Call Detail Records (CDRs)

You can configure the wireless controller to generate Call Detail Records (CDRs), which contain usage information about each wireless session per VNS. For more information on how to configure the controller to generate CDRs, refer to [Defining Accounting Methods for a WLAN Service](#) on page 289.

CDRs are located in a CDR directory on the controller. To access the CDR file, you must first back up the file on the local drive, and then upload it to a remote server. After the CDR file is uploaded to a remote server, you can work with the file to view CDRs or import the records to a reporting tool.

You can back up and upload the file on the remote server either via the Wireless Assistant (GUI) or CLI.

CDR File Naming Convention

CDRs are written to a file on the controller. The filename is based on the creation time of the CDR file with the following format: YYYYMMDDhhmmss.<ext>

- **YYYY** — Four digit year
- **MM** — Two digit month, padded with a leading zero if the month number is less than 10
- **DD** — Two digit day of the month, padded with a leading zero if the day number is less than 10
- **hh** — Two digit hour, padded with a leading zero if the hour number is less than 10
- **mm** — Two digit minute, padded with a leading zero if the minute number is less than 10
- **ss** — Two digit second, padded with a leading zero if the second number is less than 10
- **<ext>** — File extension, either .work or .dat

CDR File Types

Two types of CDR files exist in the CDR directory on the controller:

- **.work** — The active file that is being updated by the accounting system. The file is closed and renamed with the **.dat** extension when it attains its maximum size (16 MB) or it has been open for the maximum allowed duration (12 hours). You can back up and copy the **.work** file from the controller to a remote server.
- **.dat** — The inactive file that contains the archived account records. You can back up and copy the **.dat** file from the controller to a remote server.

Note



The CDR directory on the controller only has two files — a **.work** file and a **.dat** file. When the **.work** file attains its maximum size of 16 MB, or it has been open for 12 hours, it is saved as a **.dat** file. This new **.dat** file overwrites the existing **.dat** file. If you want to copy the existing **.dat** file, you must do so before it is overwritten by the new **.dat** file.

CDR File Format

A CDR file contains a sequence of CDR records. The file is a standard ASCII text file. Records are separated by a sequence of dashes followed by a line break. The individual fields of a record are reported one per line, in "field=value" format.

The following table describes the records that are displayed in a CDR file.



Note

Most of the CDR records are typical RADIUS server attributes. For more information, refer to the user manual of your RADIUS server.

Table 121: CDR Records and Their Description

CDR Records	Description
Acct-Session-ID	A unique CDR ID
User-Name	The name of the user, who was authenticated.
Filter-ID	The name of the filter list for the user.
Acct-Interim-Interval	The number of seconds between interim accounting updates.
Session-Timeout	The maximum number of seconds of service to be provided to the user before termination of the session.
Class	This field is copied from the access-accept message sent by the RADIUS server during authentication.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
Acct-Delay-Time	Indicates how many seconds the client tried to authenticate send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS (AAA), Local (Internal CP) or Remote (External CP). The field displays one of the following values: <ul style="list-style-type: none"> • 1 – AAA authentication • 2 – Internal CP authentication • 3 – External CP authentication
Framed-IP-Address	Indicates the address to be configured for the user
Connect-Info	This field is sent from the NAS to indicate the nature of the users' connection – 802.11b for Radio b/g or 802.11a for radio a.
NAS-Port-Type	Indicates RADIUS NAS Port Type is Wireless 802.11
Called-Station-ID	The Wireless AP's MAC address.
Calling-Station-ID	The client's MAC address.
Extreme Networks-AP-Serial	The AP's serial number.
Extreme Networks-AP-Name	The AP's name.
Extreme Networks-VNS-Name	The VNS name on which the session took place.
Extreme Networks-SSID	The SSID name on which the session took place.
Acct-Session-Time	The number of seconds the user has received the service.
Acct-Output-Packets	The number of packets that were sent to the port in the course of delivering this service to a framed user.
Acct-Input-Packets	The number of packets that have been received from the port over the course of this service being provided to a Framed User.

Table 121: CDR Records and Their Description (continued)

CDR Records	Description
Acct-Output-Octets	The number of octets that were sent to the port in the course of delivering the service.
Acct-Input-Octets	The number of octets that were received from the port over the course of the service.
Acct-Terminate-Cause	Indicates how the session was terminated. The field displays one of the following values: <ul style="list-style-type: none"> • 1 – User Request 4 – Idle Timeout • 5 – Session Timeout • 6 – Admin Reset • 11 – NAS Reboot • 16 – Callback • 17 – User Error
Authenticated_time	Indicates the time at which the client was authenticated. The time is in the following format: Date hh:mm:ss . For example, April 21 2008 14:50:24
Disassociation_time	Indicates the time at which the client was disassociated from the AP. The time is in the following format: Date hh:mm:ss . For example, April 21 2008 14:57:20 .

Viewing CDRs

The following is a high-level overview of how to view CDRs:

- 1 Back up the CDR files on the local drive of the controller.
- 2 Copy the CDR files from the controller to the remote server.
- 3 Unzip the file.
- 4 Download the CDR files from the remote server to view CDRs.



Note

You cannot access the CDR files directly from the CDR directory.

When you back up CDRs, both the **.work** and **.dat** files are zipped into a single **.zip** file. This **.zip** file is uploaded on the remote server. You can unzip this file from the remote server to extract the **.work** and **.dat** files.

You can back up and upload the files on the remote server either via the Wireless Assistant (GUI) or CLI.

This section describes how to back up and copy the CDR files to a remote server via the Wireless Assistant (GUI). For more information on how to copy the CDR file to the remote server via CLI, refer to the Extreme Networks ExtremeWireless *CLI Reference Guide*.

Backing Up and Copying CDR Files to a Remote Server

To Back Up and Copy the CDR Files to a Remote Server:

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

- 4 From the **Select what to backup** drop-down menu, click **CDRs only**, and then click **Backup Now**. The following window displays the backup status.

- 5 To close the window, click **Close**. The backed up file is displayed in the **Available Backups** box.



Note

The **.work** and **.dat** files are zipped into a single file.

6 To upload a backup to a Remote, in the **Copy Selected Backup > to** section, select **Remote**, then do the following:

- **Protocol** — Select the file transfer protocol you want to use to upload the backup file, SCP or FTP.
- **Server** — Type the IP address of the server where the backup will be stored.



Note

The Server Address field supports both IPv4 and IPv6 addresses.

- **User ID** — Type the user ID to log in to the server.
 - **Password** — The password to log in to the server.
 - **Confirm** — The password to confirm the password.
 - **Directory** — The directory in which you want to upload the CDR file.
 - **Filename** — Select the zipped CDR file name.
- 7 To upload a backup to Flash, in the **Copy Selected Backup > to** section, select **Flash**, then do the following:
- **Filename** — Select the zipped CDR file name.
- 8 In the **Copy Selected Backup to** section, click **Copy**. The .zip file is uploaded on to the server.
- 9 Unzip the file. The two CDR files — **.work** and **.dat** — are visible on the server.
- 10 To view CDRs, download the files.

```

-----
Acct-Session-Id = 48c937230002
User-Name = tester1
Filter-Id = Default
Acct-Interim-Interval = 1800
Session-Timeout = 0
Class = 0x000000000000
Acct-Status-Type = 2
Acct-Delay-Time = 0
Acct-Authentic = 1
Framed-IP-Address = 172.29.31.16
Connect-Info = 802.11b/g
NAS-Port-Type = Wireless-802.11
Called-Station-ID = 00:12:33:73:70:08
Calling-Station-ID = 00:0B:7D:16:46:FF
Siemens-AP-Serial = 00000012CF737033
Siemens-AP-Name = 00000012CF737033
Siemens-VNS-Name = CNL-209-AAA
Siemens-SSID = CNL-209-AAA
Acct-Session-Time = 9236
Acct-Output-Packets = 753
Acct-Input-Packets = 854
Acct-Output-Octets = 268660
Acct-Input-Octets = 329747
Acct-Terminate-Cause = 17
Authenticated_time = Sep 11 2008 11:20:03
Disassociation_time = Sep 11 2008 13:53:59

```

Figure 166: Sample .dat File

19 Performing System Administration

Performing Wireless AP Client Management
Defining Wireless Assistant Administrators and Login Groups

Performing Wireless AP Client Management

There are times when for business, service, or security reasons you want to cut the connection with a particular wireless device. You can view all the associated wireless devices, by MAC address, on a selected AP and do the following:

- Disassociate a selected wireless device from its AP. Take this action from the All Clients Report. See [Viewing All Clients](#) on page 587.
- Add a selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the AP. For more information, see [Adding Clients to a Blacklist](#) on page 615.
- Backup and restore the controller database. For more information, see the *ExtremeWireless Maintenance Guide*.

Related Links

[Viewing All Clients](#) on page 587

[Adding Clients to a Blacklist](#) on page 615



Adding Clients to a Blacklist

To create a client blacklist:

- 1 Go to **AP**.

- 2 In the left pane, click **Global > Whitelist/Blacklist**.

The screenshot shows the 'Whitelist/Blacklist' configuration page. At the top, there is a navigation bar with tabs for 'Logs', 'Reports', 'Controller', 'AP' (highlighted in purple), 'VNS', 'Radar', and 'Help'. A 'Logout' link is located in the top right corner. Below the navigation bar, the page title is 'Whitelist/Blacklist'. Underneath, there is a section titled 'MAC Addresses/OUI Prefixes:'. This section contains a large empty table on the left. To the right of the table, there is a form for adding entries, labeled 'MAC Address/OUI Prefixes:'. This form includes a text input field, an 'Add' button, and a 'Select OUI/IABs' button. Below the input field, there are two buttons: 'Select All' and 'Deselect All'. Further down, there is a 'Remove Selected' button. At the bottom of the form, there are two radio button options: 'Allow MAC only if on the MAC address list' (unselected) and 'Deny MAC address if it is on the list' (selected).

- 3 Do one of the following:
 - Type the client MAC Address or OUI Prefix and click **Add**.
 - Click **Select OUI/IABs**, and search for a client OUI/IAB by company name.
 - The Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies the client vendor or manufacturer. (Search by company name.)
 - Individual Address Block (IAB) is a block of identifiers that uniquely identify the assignee of the IAB. The purpose of the IAB is to allow organizations to purchase smaller blocks of identifiers.

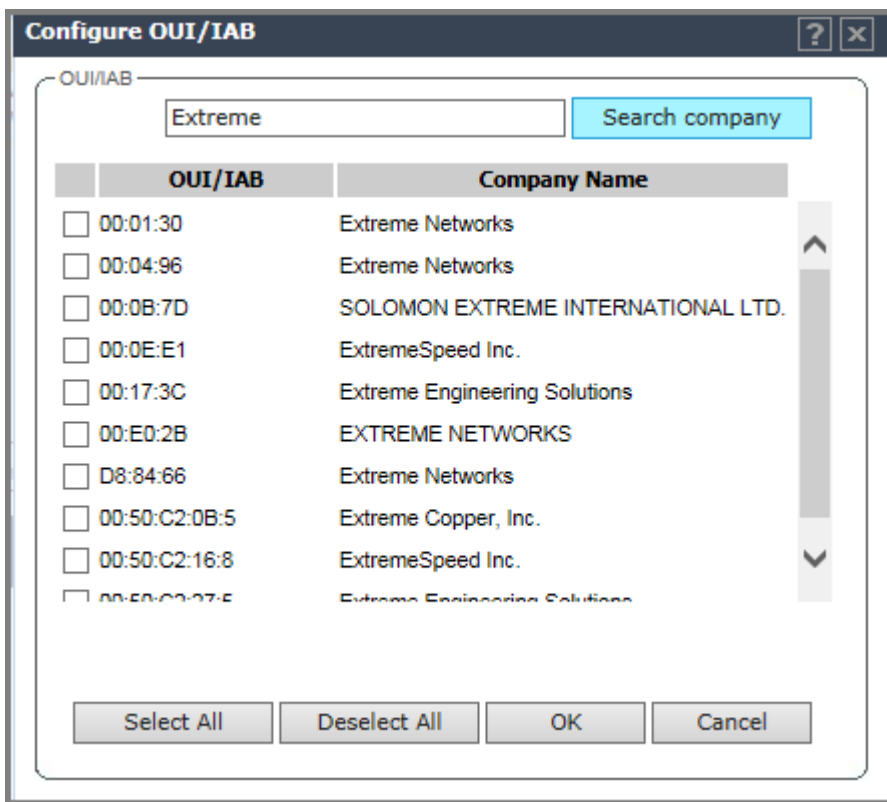


Figure 167: Searching OUI/IAB by Company Name

- Select one or more items to add to the blacklist and click **OK**.

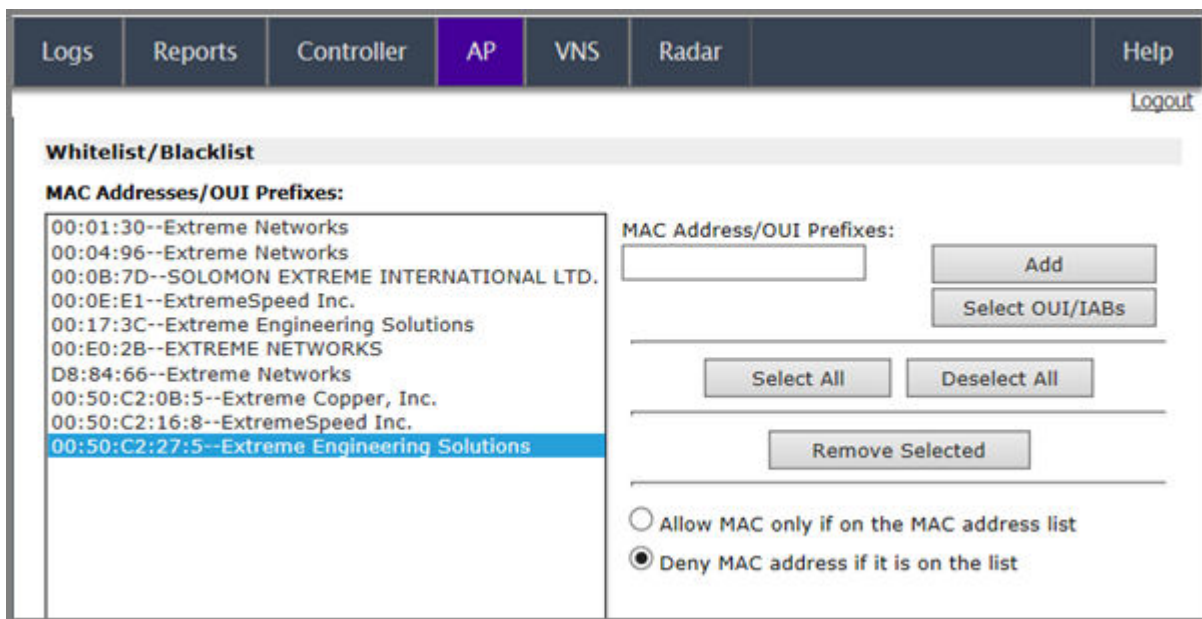


Figure 168: Example List

- To remove clients from the list, select one or more clients on the list and click **Remove Selected**.

Related Links

[Viewing Client MAC and OUI](#) on page 591

[Viewing All Clients](#) on page 587

Defining Wireless Assistant Administrators and Login Groups

You can define the login user names and passwords for administrators that have access to the Wireless Assistant. You can also assign them to a login group — as full administrators, read-only administrators, or as GuestPortal managers. For each user added, you can define and modify a user ID and password.

- **Full administrators** — Users assigned to this login group have full administrator access rights on the controller. Full administrators can manage all aspects of the controller, including GuestPortal user accounts.
- **Read-only administrators** — Users assigned to this login group have read-only access rights on the controller, including the GuestPortal user accounts.
- **GuestPortal managers** — Users assigned to this login group can only manage GuestPortal user accounts. Any user who logs on to the controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the Wireless Assistant.



Note

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

To add a controller administrator to a login group:

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

- 2 From the left pane, click **Administration** > **Login Management**.

The following screen appears:

The screenshot shows the 'Local Authentication' configuration interface. It features a left-hand navigation pane with three user group options: 'Full Administrator' (highlighted), 'Read-only Administrator', and 'GuestPortal Manager'. The main content area is split into two sections: 'Add User' and 'Modify User'. The 'Add User' section includes a dropdown menu for 'Group' (currently set to 'Full Administrator'), and three input fields for 'User ID', 'Password', and 'Confirm Password', with an 'Add User' button below. The 'Modify User' section includes an input field for 'User ID' (pre-filled with 'admin'), and three input fields for 'Password', 'Confirm Password', and 'Reset', with buttons for 'Change Password', 'Remove user', and 'Reset'. At the bottom, the 'Authentication mode' is set to 'Local, RADIUS', with 'Configure' and 'Save' buttons.

- 3 In the **Group** drop-down list, click one of the following:
- **Full Administrator** — Users assigned to this login group have full administrator access rights on the controller.
Full administrators can manage GuestPortal user accounts.
 - **Read-only Administrator** — Users assigned to this login group have read-only access rights on the controller.
Read-only administrators have read access to the GuestPortal user accounts.
 - **GuestPortal Manager** — Users assigned to this login group can only manage GuestPortal user accounts. Any user who logs on to the controller and is assigned to this group can only access the **GuestPortal Guest Administration** page of the wireless assistant. For more information, see [Performing System Administration](#) on page 615.
- 4 In the **User ID** box, type the user ID for the new user. A user ID can only be used once, in only one category.
- 5 In the **Password** box, type the password for the new user.
- 6 **In the Confirm Password, re-type the password.**

- 7 Click **Add User**. The new user is added to the appropriate login group list.

Related Links

[Modifying Admin Password](#) on page 620

[Removing Administrator](#) on page 620

Modifying Admin Password

To modify a controller administrator password:

- 1 Go to **Controller**.
- 2 In the left pane, click **Administration** > **Login Management**.
- 3 Click the user whose password you want to modify.
- 4 In the **Password** box, type the new password for the user.
- 5 Under **Confirm Password** re-type the new password.
- 6 To change the password, click **Change Password**.

Removing Administrator

To remove a controller administrator:

- 1 Go to **Controller**.
- 2 In the left pane, click **Administration** > **Login Management**. The **Local Authentication** tab is displayed.
- 3 Click the user you want to remove.
- 4 Click **Remove user**. The user is removed from the list.

20 Logs, Traces, Audits and DHCP Messages

ExtremeWireless Appliance Messages

Working with Logs

Viewing Wireless AP Traces

Viewing Audit Messages

Viewing the DHCP Messages

Viewing the NTP Messages

Viewing Software Upgrade Messages

Viewing Configuration Restore/Import Messages

ExtremeWireless Appliance Messages

The ExtremeWireless Appliance generates four types of messages:

- **Logs (including alarms)** – Messages that are triggered by events
- **Traces** – Messages that display activity by component, for system debugging, troubleshooting, and internal monitoring of software

Caution



In order for the **Debug Info** option on the **Wireless AP Traces** screen to return trace messages, this option must be enabled while Wireless AP debug commands are running. To do so, you need to run a Wireless AP CLI command to turn on a specific Wireless AP debug. Once the CLI command is run, select the **Debug Info** option, and then click **Retrieve Traces**. For more information, see Extreme Networks *ExtremeWireless CLI Reference Guide*. Because Wireless AP debugging can affect the normal operation of Wireless AP service, enabling debugging is not recommended unless specific instructions are provided.

- **Audits** – Messages that record administrative changes made to the system
- **DHCP** – Messages that record service events

Working with Logs

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

- Controller logs
- Wireless AP logs
- Login logs

Log Severity Levels

Log messages are classified at four levels of severity:

- Information (the activity of normal operation)
- Minor (alarm)
- Major (alarm)
- Critical (alarm)

The alarm messages (minor, major or critical log messages) are triggered by activities that meet certain conditions that should be known and dealt with. The following are examples of events on the wireless controller that generate an alarm message:

- Reboot due to failure
- Software upgrade failure on the wireless controller
- Software upgrade failure on the wireless AP
- Detection of rogue access point activity without valid ID
- Availability configuration not identical on the primary and secondary wireless controller

If SNMP is enabled on the wireless controller, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions.

Note



The log statements **Low water mark level was reached** and **Incoming message dropped, because of the rate limiting mechanism** indicate that there is a burst of log messages coming to the event server and the processing speed is slower than the incoming rate of log messages. These messages do not indicate that the system is impaired in any way.

Viewing the Wireless Controller Logs

To view wireless controller logs:

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

- Click **EWC Events**. The log screen displays and the events are displayed in chronological order.

The screenshot shows the EWC Events log screen. The navigation menu includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The 'Logs' menu is active. Below the menu, there are filters for 'Severity' (Critical, Major, Minor, Info, All) and a table of log messages. The table has columns for 'Timestamp', 'Type', 'Component', and 'Log Message'. Two messages are shown, both with a 'Critical' type and 'CLI' component, with timestamps '03/03/14 05:57:11' and '03/03/14 04:18:53'. The log messages are 'USER GENERATED EVENT: Critical Logs During Smoke Test - lab-422-g-1403030332'. At the bottom, there are navigation buttons: 'First', 'Previous', '1', 'Next', 'Last', 'Tech Support', 'Export', and 'Refresh'.

- To sort the events by Timestamp, Type, or Component, click the appropriate column heading.
- To filter the events by severity, Critical, Major, Minor, Info, and All, click the appropriate log severity.
- To refresh the log screen, click **Refresh**.
- To export the log screen, click **Export**. The **File Download** dialog is displayed.
- Do one of the following:
 - To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.



Note

The component 'Langley' is the term for the inter-process messaging infrastructure on the wireless controller.

Viewing Wireless Controller Station Logs

To view wireless controller station logs:

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

- Click **ewc: Station Events**. The Station Events screen displays and the events are displayed in chronological order.



Note

Station log generation is controlled by the “Report station events on controller” checkbox on the wireless **Controller > Logs > Logs Configuration** page.

lab-422-g - Logs - Station Event Log

Showing 1 to 9 of 9 entries

Search:

Timestamp	Event Type	Station MAC Address	Station IP Address	AP Name	AP Name (From)	BSSID
03/03/14 06:09:55	Authentication	24:77:03:E6:CC:34	-	C4110 - ap2 - AP3620	-	00:1A:E8:14:2A:39
03/03/14 06:09:55	State Change	24:77:03:E6:CC:34	-	-	-	00:1A:E8:14:2A:39
03/03/14 06:09:40	Roam	24:77:03:E6:CC:34	-	C4110 - ap2 - AP3620	-	00:1A:E8:14:2A:39
03/03/14 06:08:58	State Change	24:77:03:E6:CC:34	10.219.46.102	-	-	00:1A:E8:14:2A:39
03/03/14 06:08:57	Authentication	24:77:03:E6:CC:34	-	C4110 - ap2 - AP3620	-	00:1A:E8:14:2A:39
03/03/14 06:08:57	State Change	24:77:03:E6:CC:34	-	-	-	00:1A:E8:14:2A:39
03/03/14 06:08:57	State Change	24:77:03:E6:CC:34	-	-	-	00:1A:E8:14:2A:39
03/03/14 06:08:57	MBA Accepted	24:77:03:E6:CC:34	-	C4110 - ap2 - AP3620	-	00:1A:E8:14:2A:39
03/03/14 06:08:57	Registration	24:77:03:E6:CC:34	-	C4110 - ap2 - AP3620	-	00:1A:E8:14:2A:39

Showing 1 to 9 of 9 entries

† To sort by multiple columns, click the first column, hold down the SHIFT key, and then click the next column. As many columns as you wish can be added to the sort.

Data as of Mar 03, 2014 01:35:46 pm

The table is sortable on all column (ascending and descending), if you close this log window and open it again within the same GUI session, it remembers you previous column sorting option, plus it has multi-column sorting.

- To sort by multiple columns, click the first column, hold down the **[Shift]** key, and then click the next column. As many columns as you wish can be added to the sort.
- Click on MAC addresses in Station MAC Address column to see up-to-date details about the particular station.
- Click the **Search** box and enter text. The information is filtered automatically as you type and only lines which match this text in any column (on all pages) are displayed.
- Click **Refresh** to refresh the log. This log doesn't refresh automatically (the same as other logs).
- To export the Station log screen, click **Export**. The File Download dialog is displayed. Do one of the following:
 - To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

- 8 Click **Close** to close this log window.

Viewing Wireless AP Logs

To View Wireless AP Logs:

- 1 From the top menu, click **Logs**.
- 2 Click **AP: Logs**. The **wireless AP Log** screen displays and the events are displayed in chronological order.

Wireless AP	EWC time	Sev	AP-time/up-time : Log Messages
C5110 - ap1 - AP3765e	11/16/15 14:01:51	Critical	11/16/15 19:00:52: AccessPoint Rebooting due to: Software Image Upgrade

- 3 In the **Wireless AP** list, click a Wireless AP to view the log events for that particular Wireless AP.
- 4 To sort the events by **EWC time** or **Sev** (Severity), click the appropriate column heading.
- 5 To filter the events by severity, **Critical**, **Major**, **Minor**, **Information**, and **All**, click the appropriate log severity.
- 6 To refresh the log screen, click **Refresh**.
- 7 To export the logs, click **Export**. The **File Download** dialog is displayed.
- 8 Do one of the following:
 - To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Viewing Login Logs

To View Administrator Login Logs:

- 1 From the top menu, click **Logs**.
- 2 Click **Login** . The **Login** screen displays and the login events are displayed in chronological order.

Timestamp	Auth Message
03/03/14 13:33:00	lab-422-g gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
03/03/14 13:33:00	lab-422-g pam_radauth[2038]: (www) User [admin] has been rejected in authentication on radius server [192.168.3.158].
03/03/14 13:25:49	lab-422-g gui_s_mgr: (pam_unix) session closed for user admin
03/03/14 13:16:49	lab-422-g gui_s_mgr: (pam_unix) session closed for user admin
03/03/14 12:24:27	lab-422-g gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
03/03/14 12:24:27	lab-422-g pam_radauth[2038]: (www) User [admin] has been rejected in authentication on radius server [192.168.3.158].
03/03/14 12:19:49	lab-422-g gui_s_mgr: (pam_unix) session closed for user admin
03/03/14 11:22:11	lab-422-g gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
03/03/14 11:22:11	lab-422-g pam_radauth[2038]: (www) User [admin] has been rejected in authentication on radius server [192.168.3.158].
03/03/14 10:24:29	lab-422-g gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
03/03/14 10:24:29	lab-422-g pam_radauth[2038]: (www) User [admin] has been rejected in authentication on radius server [192.168.3.158].
03/03/14 09:47:34	lab-422-g gui_s_mgr: (pam_unix) session closed for user admin
03/03/14 09:07:01	lab-422-g gui_s_mgr: (pam_unix) session opened for user admin by (uid=0)
03/03/14 09:07:01	lab-422-g pam_radauth[2038]: (www) User [admin] has been rejected in authentication on radius server [192.168.3.158].
03/03/14 06:07:55	lab-422-g login: (pam_unix) session opened for user root by (uid=0)
03/03/14 06:07:55	lab-422-g pam_radauth[2860]: (login) User [root] has been rejected in authentication on radius server [192.168.3.158].

140 messages Refresh

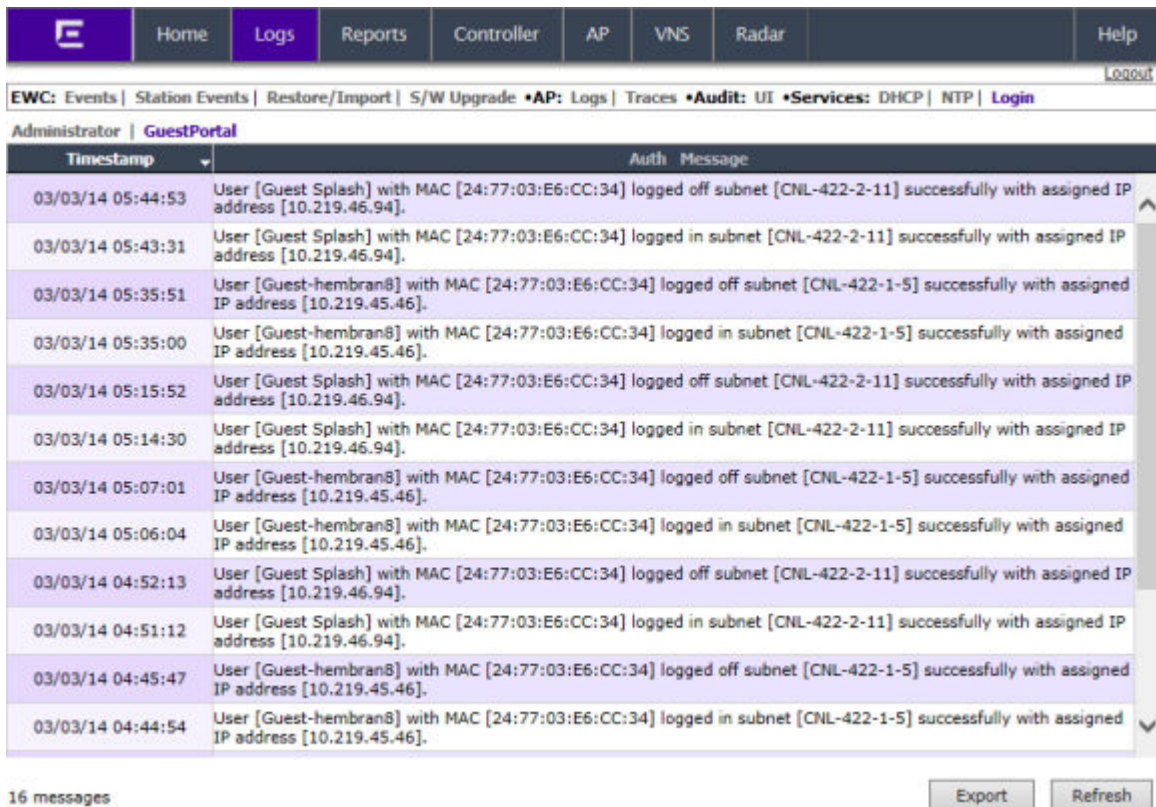
- 3 To refresh the **Login** screen, click **Refresh**.

Working with GuestPortal Login Logs

To view GuestPortal login logs:

- 1 From the top menu, click **Logs**.
- 2 Click **Login** . The **Login** screen displays and the login events are displayed in chronological order.

- 3 Click **GuestPortal**. The GuestPortal login events are displayed in chronological order.



The screenshot shows the GuestPortal interface with a navigation menu at the top. The 'Logs' menu item is selected. Below the navigation, there are several tabs: 'EWC: Events', 'Station Events', 'Restore/Import', 'S/W Upgrade', 'AP: Logs', 'Traces', 'Audit: UI', 'Services: DHCP', 'NTP', and 'Login'. The 'AP: Logs' tab is active, and the 'GuestPortal' sub-tab is selected. The main content area displays a table of 16 messages. The table has two columns: 'Timestamp' and 'Auth Message'. The messages are sorted chronologically, with the most recent at the top. Each message entry includes a timestamp and a detailed log message describing a user's login or logout event, including the user type (Guest Splash or Guest-hembran8), MAC address, and subnet information.

Timestamp	Auth Message
03/03/14 05:44:53	User [Guest Splash] with MAC [24:77:03:E6:CC:34] logged off subnet [CNL-422-2-11] successfully with assigned IP address [10.219.46.94].
03/03/14 05:43:31	User [Guest Splash] with MAC [24:77:03:E6:CC:34] logged in subnet [CNL-422-2-11] successfully with assigned IP address [10.219.46.94].
03/03/14 05:35:51	User [Guest-hembran8] with MAC [24:77:03:E6:CC:34] logged off subnet [CNL-422-1-5] successfully with assigned IP address [10.219.45.46].
03/03/14 05:35:00	User [Guest-hembran8] with MAC [24:77:03:E6:CC:34] logged in subnet [CNL-422-1-5] successfully with assigned IP address [10.219.45.46].
03/03/14 05:15:52	User [Guest Splash] with MAC [24:77:03:E6:CC:34] logged off subnet [CNL-422-2-11] successfully with assigned IP address [10.219.46.94].
03/03/14 05:14:30	User [Guest Splash] with MAC [24:77:03:E6:CC:34] logged in subnet [CNL-422-2-11] successfully with assigned IP address [10.219.46.94].
03/03/14 05:07:01	User [Guest-hembran8] with MAC [24:77:03:E6:CC:34] logged off subnet [CNL-422-1-5] successfully with assigned IP address [10.219.45.46].
03/03/14 05:06:04	User [Guest-hembran8] with MAC [24:77:03:E6:CC:34] logged in subnet [CNL-422-1-5] successfully with assigned IP address [10.219.45.46].
03/03/14 04:52:13	User [Guest Splash] with MAC [24:77:03:E6:CC:34] logged off subnet [CNL-422-2-11] successfully with assigned IP address [10.219.46.94].
03/03/14 04:51:12	User [Guest Splash] with MAC [24:77:03:E6:CC:34] logged in subnet [CNL-422-2-11] successfully with assigned IP address [10.219.46.94].
03/03/14 04:45:47	User [Guest-hembran8] with MAC [24:77:03:E6:CC:34] logged off subnet [CNL-422-1-5] successfully with assigned IP address [10.219.45.46].
03/03/14 04:44:54	User [Guest-hembran8] with MAC [24:77:03:E6:CC:34] logged in subnet [CNL-422-1-5] successfully with assigned IP address [10.219.45.46].

16 messages

Export Refresh

- 4 To export the GuestPortal log information, click **Export**. The **File Download** dialog is displayed.
- 5 Do one of the following:
- To open the log file, click **Open**.
 - To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Working with a Tech Support File

- 1 To generate a Tech Support file, click **Logs** from the top menu.
The **Logs & Traces** screen displays.
- 2 Ensure that **EWC:Events** is selected.

- 3 Click the **Tech Support** button at the bottom of the page.
The **Generate Tech Support File** screen displays.

- 4 Select the parameters for the tech support file:
 - **Wireless Controller**
 - **Wireless AP**
 - **Logs**
 - **All**
 - **No Stats** – If **Wireless AP** is selected, select this checkbox to include or exclude Wireless AP statistics in the tech support file.
- 5 Click **Generate New Tech Support File**.
A warning message is displayed informing you that this operation may temporarily affect system performance.
- 6 Click **OK** to continue.
The tech support file generation status is displayed.
- 7 When the file generation has completed, click **Close**.
- 8 To download the last generated Tech Support file, click **Logs** from the top menu.
The **Logs & Traces** screen displays.
- 9 Ensure that the **EWC** tab is selected.
- 10 Click the **Tech Support** button at the bottom of the page.
The **Generate Tech Support File** screen displays.
- 11 Click **Download Last Tech Support File**.
The **File Download** dialog is displayed.
- 12 Click **Save**.
The **Save as** window is displayed.
- 13 Navigate to the location you want to save the generated tech support file, and then click **Save**.
- 14 To delete a Tech Support file, click **Logs** from the top menu.
The **Logs & Traces** screen displays.
- 15 Ensure that the **EWC** tab is selected.

- 16 Click the **Tech Support** button at the bottom of the page.
The **Generate Tech Support File** screen displays.
- 17 Click **List All Tech Support Files**.
- 18 In the drop-down list, click the tech support file you want to delete.
The tech support file is deleted.
- 19 Click **Close**.

Viewing Wireless AP Traces

To view wireless AP traces:

- 1 From the top menu, click **Logs**.
- 2 Click **AP: Traces**.

The **Wireless AP** trace screen displays.

- 3 In the **Wireless AP** list, click the Wireless AP whose trace messages you want to view.
- 4 Click **Retrieve Traces**. Depending on the browser, the **File Download** dialog appears.
- 5 Click **Save** and navigate to the location on your computer that you want to save the Wireless AP trace report.
The file is saved as a .tar file.
- 6 To view the file, unpack the .tar file.

Viewing Audit Messages

To View Audit Messages:

- 1 From the top menu, click **Logs**.
- 2 Click **Audit: UI**. The **Audit** screen displays and the events are displayed in chronological order.

Timestamp	User	Section	Page	Audit Message
03/03/14 12:10:28	admin	Sys Mgmt	SW Maint.	Maintenance task: export of [cdrs] to local
03/03/14 12:10:27	admin	CLI_system_m anagement	backup	SUCCESS to complete backup/export: backup/export file: lab-422-g.03032014.121027.
03/03/14 05:26:15	admin	ap	named_ap	AP 0500008043050317 configuration changed: static_mtu [1200],
03/03/14 05:25:45	admin	ap	named_ap	AP 0500008043050317 configuration changed: secure_tunnel_mode [2],
03/03/14 04:56:45	admin	ap	named_ap	AP 0500008043050317 configuration changed: static_mtu [1100],
03/03/14 04:56:45	admin	ap	named_ap	AP 0500008043050317 configuration applied:
03/03/14 04:39:13	admin	ap	named_ap	AP 1406000708420000 configuration changed: static_mtu [1200],
03/03/14 04:38:43	admin	ap	named_ap	AP 1406000708420000 configuration changed: secure_tunnel_mode [2],
03/03/14 04:21:53	admin	ap	named_ap	AP 1406000708420000 configuration changed: static_mtu [1100],
03/03/14 04:21:53	admin	ap	named_ap	AP 1406000708420000 configuration applied:
03/03/14 04:21:39	admin	vns	wlans	AP list has changed for WLANS[CNL-422-0-0] to [{"status": 0, "wds_bridge": 0, "name": "C4110 - ap1 - AP4102", "radios": [{"radio_index": 1, "wds_role": 0, "assoc": 1, "load_balance_group_assigned": 0}, {"radio_index": 2, "wds_role": 0, "assoc": 0, "load_balance_group_assigned": 0}], "wds_backup_parent": "", "foreign": 0, "wds_pref_parent": "", "role": 0, "serial": "0002000609223321"}, {"status": 0, "wds_bridge": 0, "name": "C4110 - ap2 - AP3620", "radios": [{"wds_role": 0, "protocol": 20, "assoc": 0, "load_b
03/03/14 04:21:39	admin	vns	wlans	AP list has changed for WLANS[CNL-422-0-0] to [{"status": 0, "wds_bridge": 0, "name": "C4110 - ap1 - AP4102", "radios": [{"radio_index": 1, "wds_role": 0, "assoc": 1, "load_balance_group_assigned": 0}, {"radio_index": 2, "wds_role": 0, "assoc": 0, "load_balance_group_assigned": 0}], "wds_backup_parent": "", "foreign": 0, "wds_pref_parent": "", "role": 0, "serial": "0002000609223321"}, {"status": 0, "wds_bridge": 0, "name": "C4110 - ap2 - AP3620", "radios": [{"wds_role": 0, "protocol": 20, "assoc": 0, "load_b

34 messages To sort by multiple columns, click the first column, hold down the SHIFT key then click the next column. Export Refresh

- 3 To sort the events by **Timestamp, User, Section, or Page**, click the appropriate column heading.
- 4 To refresh the audit screen, click **Refresh**.
- 5 To export the audit screen, click **Export**. The **File Download** dialog is displayed.
- 6 Do one of the following:
 - To open the audit file, click **Open**.
 - To save the audit file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Viewing the DHCP Messages

To View Messages:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.

- 2 Click **Service: DHCP**. The DHCP message screen displays and the events are displayed in chronological order.

Timestamp	DHCP Message
03/03/14 11:09:55	dhcpcd: DHCPACK on 10.219.46.102 to 24:77:03:e6:cc:34 (MU3) via csi18
03/03/14 11:09:55	dhcpcd: DHCPREQUEST for 10.219.46.102 from 24:77:03:e6:cc:34 (MU3) via csi18
03/03/14 11:09:55	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:09:55	dhcpcd: DHCPACK on 10.219.46.102 to 24:77:03:e6:cc:34 (MU3) via csi18
03/03/14 06:09:55	dhcpcd: DHCPREQUEST for 10.219.46.102 from 24:77:03:e6:cc:34 (MU3) via csi18
03/03/14 06:07:47	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:07:41	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:01:21	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:01:18	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:01:11	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:01:06	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:01:02	dhcpcd: Wrote 13 leases to leases file.
03/03/14 06:01:02	dhcpcd: lease 10.219.42.254: no subnet.
03/03/14 05:57:45	dhcpcd: Wrote 14 leases to leases file.
03/03/14 05:53:27	dhcpcd: DHCPACK on 10.219.46.102 to 24:77:03:e6:cc:34 (MU3) via csi18
03/03/14 05:53:27	dhcpcd: DHCPREQUEST for 10.219.46.102 from 24:77:03:e6:cc:34 via csi18
03/03/14 05:49:50	dhcpcd: DHCPACK on 10.219.47.126 to 24:77:03:e6:cc:34 (MU3) via csi22
03/03/14 05:49:50	dhcpcd: DHCPREQUEST for 10.219.47.126 from 24:77:03:e6:cc:34 via csi22
03/03/14 05:48:15	dhcpcd: DHCPACK on 10.219.47.118 to 24:77:03:e6:cc:34 (MU3) via csi21
03/03/14 05:48:15	dhcpcd: DHCPREQUEST for 10.219.47.118 from 24:77:03:e6:cc:34 via csi21
03/03/14 05:46:33	dhcpcd: DHCPACK on 10.219.47.110 to 24:77:03:e6:cc:34 (MU3) via csi20

165 messages Refresh

- 3 To sort the events by **timestamp**, click **Timestamp**.
- 4 To refresh the DHCP message screen, click **Refresh**.

Viewing the NTP Messages

To view NTP messages:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.

- 2 Click **Service: NTP**. The NTP message screen displays and the events are displayed in chronological order.

Timestamp	NTP Message
03/03/14 13:24:00	ntpd[2783]: kernel time sync status change 4001
03/03/14 12:49:50	ntpd[2783]: kernel time sync status change 0001
03/03/14 12:32:44	ntpd[2783]: kernel time sync status change 4001
03/03/14 10:33:05	ntpd[2783]: kernel time sync status change 0001
03/03/14 10:07:25	ntpd[2783]: kernel time sync status change 4001
03/03/14 06:12:44	ntpd[2783]: Listening on interface #23 csi16, 10.219.43.1#123 Enabled
03/03/14 06:12:44	ntpd[2783]: Listening on interface #22 csi7, 10.219.42.1#123 Enabled
03/03/14 06:12:44	ntpd[2783]: Listening on interface #21 csi2, 10.219.41.1#123 Enabled
03/03/14 06:12:44	ntpd[2783]: Listening on interface #20 csi1, 10.219.40.1#123 Enabled
03/03/14 06:10:59	ntpd[2783]: kernel time sync status change 0001
03/03/14 06:10:59	ntpd[2783]: synchronized to 192.168.3.100, stratum 14
03/03/14 06:07:43	ntpd[2783]: kernel time sync status 0040
03/03/14 06:07:43	ntpd[2783]: Listening on interface #19 tap0, 172.31.0.17#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #18 csi22, 10.219.47.121#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #17 csi21, 10.219.47.113#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #16 csi20, 10.219.47.105#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #15 csi19, 10.219.47.97#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #14 csi18, 10.219.46.97#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #13 csi17, 10.219.46.89#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #12 csi15, 10.219.46.73#123 Enabled
03/03/14 06:07:43	ntpd[2783]: Listening on interface #11 csi13, 10.219.45.57#123 Enabled

109 messages Refresh

- 3 To sort the events by timestamp, click **Timestamp**.
- 4 To refresh the NTP message screen, click **Refresh**.

Viewing Software Upgrade Messages

The **S/W Upgrade** tab displays the most recent upgrade actions, either success or failure, and the operating system patch history. Some examples of the upgrade actions that can be displayed are:

- FTP failure during backup of system image
- Configuration reset failure
- Configuration export failure
- Configuration import details

To view software upgrade messages:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.

- 2 Click the **S/W Upgrade** tab. The software upgrade message screen displays.

Date	Type	Version
Mon Mar 3 04:03:36 EST 2014	Upgraded	09.01.01.0207T
Thu Feb 20 18:27:12 EST 2014	Installed	09.01.01.0196
Thu Feb 20 18:26:54 EST 2014	Installed	OS-9_1_0-5

3 messages To sort by multiple columns, click the first column, hold down the SHIFT key then click the next column. Export Refresh

- 3 Do the following:
- To view software upgrade messages, click **Detail**.
 - To view the operating system history, click **History**.
- 4 To refresh the screen, click **Refresh**.
- 5 To export the software upgrade messages or operating system history, click **Export**. The **File Download** dialog is displayed.
- 6 Do one of the following:
- To open the file, click **Open**.
 - To save the file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

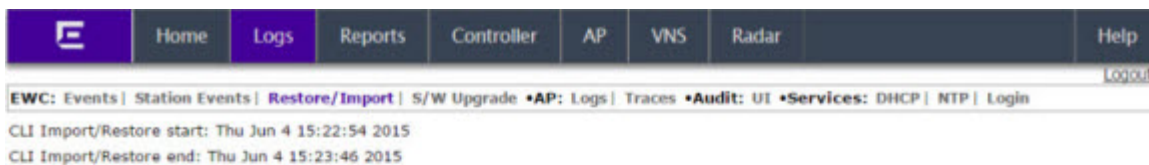
Viewing Configuration Restore/Import Messages

The **Restore/Import** tab displays the most recent configuration restore/import results.

To View Restore/Import Messages:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.

- 2 Click the **Restore/Import** tab. The restore/import message screen displays.



- 3 To refresh the restore/import message screen, click **Refresh**.
- 4 To export the restore/import message screen, click **Export**. The **File Download** dialog is displayed.
- 5 Do one of the following:
 - To open the file, click **Open**.
 - To save the file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

21 Working with GuestPortal Administration

About GuestPortals
Adding New Guest Accounts
Enabling or Disabling Guest Accounts
Editing Guest Accounts
Removing Guest Accounts
Importing and Exporting a Guest File
Viewing and Printing a GuestPortal Account Ticket
Working with the Guest Portal Ticket Page
Configuring Guest Password Patterns
Configuring Web Session Timeouts

About GuestPortals

A GuestPortal provides wireless device users with temporary guest network services. A GuestPortal is serviced by a GuestPortal-dedicated VNS. The GuestPortal-dedicated VNS is configured by an administrator with full administrator access rights. For more information, see [Creating a GuestPortal VNS](#) on page 429.

A GuestPortal administrator is assigned to the GuestPortal Manager login group and can only create and manage guest user accounts — a GuestPortal administrator cannot access any other area of the Wireless Assistant. For more information, see [Defining Wireless Assistant Administrators and Login Groups](#) on page 618.

From the **GuestPortal Guest Administration** page of the Wireless Assistant, you can add, edit, configure, and import and export guest accounts.

Adding New Guest Accounts

To add a new guest account:

1 Do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
 - From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
 - In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
 - Click the **Auth & Acct** tab.
 - Make sure the Mode is set to Guest Splash and then click **Configure**. The Configuration page displays.
 - In the **Guest Splash** section, click **Manage Guest Users**.
 - The **Guest Splash Administration** screen displays.

Note

You have 3 minutes to add new guest user accounts. If that time expires, close the **Guest Splash Administration** screen and click **Manage Guest Users** again. You can also increase the **Start date** time to be within 3 minutes of the current network time.

Search

User Name:

Print Ticket for Selected Account

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

Account Management

Account Enable/Disable

File Management

- 2 In the **Account Management** section, click **Add Guest Account**. The **Add Guest User** screen displays.

- 3 To enable the new guest account, select the **Enabled** checkbox. For more information, see [Enabling or Disabling Guest Accounts](#) on page 638.
- 4 In the **Credentials** section, do the following:
- **User Name** — Type a user name for the person who will use this guest account.
 - **User ID** — Type a user ID for the person who will use this guest account. The default user ID can be edited.
 - **Password** — Type a password for the person who will use this guest account. The default password can be edited.

Toggle between **Mask/Unmask** to hide or see the password.
 - **Description** — Type a brief description for the new guest account.
- 5 In the **Account Settings** section, do the following:
- **Start date** — Specify the start date and time for the new guest account.
 - **Account lifetime** — Specify the account lifetime, in days, for the new guest account. The default **0** value specifies no limit to the account lifetime. Only a user with administrative privileges can change the value of the Account lifetime.
- 6 In the **Session Settings** section, do the following:
- **Session lifetime** — Specify a session lifetime, in hours, for the new guest account. The default **0** value specifies no limit to the session lifetime. The session lifetime is the allowed cumulative total in hours spent on the network during the account lifetime.
 - **Start Time** — Specify a start time for the session for the new guest account.
 - **End Time** — Specify an end time for the session for the new guest account.
- 7 To save your changes, click **OK**.

Enabling or Disabling Guest Accounts

A guest account must be enabled in order for a wireless device user to use the guest account to obtain guest network services.

When a guest account is disabled, it remains in the database. A disabled guest account cannot provide access to the network.

To Enable or Disable Guest Accounts:

- 1 Do one of the following:
 - If you have GuestPortal Manager rights, log onto the controller.
 - If you have full administrator rights:
 - From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
 - In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
 - Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
 - In the **Guest Splash** section, click **Manage Guest Users**.
 - The **Guest Splash Administration** screen displays.

The screenshot shows the Guest Splash Administration interface. At the top, there is a search bar with the text "Search" and "User Name:" followed by an input field and a "Search" button. To the right of the search bar is a button labeled "Print Ticket for Selected Account". Below the search bar is a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data. Below the table are three groups of buttons: "Account Management" (Add Guest Account, Edit Selected Accounts, Remove Selected Accounts), "Account Enable/Disable" (Enable Selected Accounts, Disable Selected Accounts), and "File Management" (Import Guest File, Export Guest File).

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

- 2 In the guest account list, select the checkbox next to the user name of the guest account that you want to enable or disable.
- 3 In the **Account Enable/Disable** section, click **Enable Selected Accounts** or **Disable Selected Accounts** accordingly. A dialog is displayed requesting you to confirm your selection.
- 4 Click **Ok**. A confirmation message is displayed in the **Guest Splash Administration** screen footer.

Editing Guest Accounts

An already existing guest account can be edited.

To Edit a Guest Account:

- 1 Do one of the following:
 - If you have GuestPortal Manager rights, log onto the controller.
 - If you have full administrator rights:
 - From the top menu, click **VNS**.
 - In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services configuration** window for that service displays.
 - Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
 - In the **Guest Splash** section, click **Manage Guest Users**.
 - The **Guest Splash Administration** screen displays.

The screenshot shows the Guest Portal Administration interface. At the top, there is a search bar with the label "Search" and a "Search" button. Below the search bar is a "User Name:" input field and a "Search" button. To the right of the search bar is a button labeled "Print Ticket for Selected Account". Below the search bar is a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data:

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

Below the table are three sections of buttons:

- Account Management:** Add Guest Account, Edit Selected Accounts, Remove Selected Accounts
- Account Enable/Disable:** Enable Selected Accounts, Disable Selected Accounts
- File Management:** Import Guest File, Export Guest File

- 2 In the guest account list, select the checkbox next to the user name of the guest account that you want to edit.
- 3 In the **Account Management** section, click **Edit Selected Accounts**.
- 4 Edit the guest account accordingly. For more information on guest account properties, see [Adding New Guest Accounts](#) on page 635.
- 5 To save your changes, click **OK**. A confirmation message is displayed in the **Guest Splash Administration** screen footer.

Removing Guest Accounts

An already existing guest account can be removed from the database.

- 1 To remove a guest account, do one of the following:
 - If you have GuestPortal Manager rights, log onto the controller.
 - If you have full administrator rights:
 - From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
 - In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
 - Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
 - In the **Guest Splash** section, click **Manage Guest Users**. The **Guest Splash Administration** screen displays.

The screenshot shows the Guest Splash Administration interface. At the top, there is a search bar with the text "Search" and "User Name:" followed by a "Search" button. To the right is a button labeled "Print Ticket for Selected Account". Below this is a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data:

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

Below the table are three groups of buttons:

- Account Management:** Add Guest Account, Edit Selected Accounts, Remove Selected Accounts
- Account Enable/Disable:** Enable Selected Accounts, Disable Selected Accounts
- File Management:** Import Guest File, Export Guest File

- 2 In the guest account list, select the checkbox next to the user name of the guest account that you want to remove.
- 3 In the **Account Management** section, click **Remove Selected Accounts**.
A dialog is displayed requesting you to confirm your removal.
- 4 Click **OK**.
A confirmation message is displayed in the **Guest Splash Administration** screen footer.

Importing and Exporting a Guest File

To help administrators manage large numbers of guest accounts, you can import and export .csv (comma separated value) guest files for the controller.

The following describes the column values of the .csv guest file.

Table 122: Guest Account Import and Export .csv File Values

Column	Value
A	User ID
B	User name
C	Password
D	Description
E	Account activation date
F	Account lifetime, measured in days
G	Session lifetime, measured in hours
H	Is the account enabled (1) or disabled (0)
I	Time of day, start time
J	Time of day, duration
K	Total session used time, measured in seconds. A user session starts when the guest user is authenticated, and ends when the guest user is disassociated.
L	Is the guest user account synchronized on a secondary controller in an availability pair, yes (1) no (0)

- 1 To export a guest file, do one of the following:
 - If you have GuestPortal Manager rights, log onto the controller.
 - If you have full administrator rights:
 - From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
 - In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
 - Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
 - In the **Guest Splash** section, click **Manage Guest Users**.

The **Guest Splash Administration** screen displays.

The screenshot shows the Guest Splash Administration interface. At the top, there is a search bar with a 'Search' button and a 'Print Ticket for Selected Account' button. Below this is a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data:

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

Below the table, there are three main sections of buttons:

- Account Management:** Add Guest Account, Edit Selected Accounts, Remove Selected Accounts
- Account Enable/Disable:** Enable Selected Accounts, Disable Selected Accounts
- File Management:** Import Guest File, Export Guest File

- 2 In the **File Management** section, click **Export Guest File**.
A **File Download** dialog is displayed.
- 3 Click **Save**.
The **Save As** dialog is displayed.
- 4 Name the guest file, and then navigate to the location where you want to save the file.
By default, the exported guest file is named `exportguest.csv`.
- 5 Click **Save**.
The **File Download** dialog is displayed as the file is exported.
- 6 Click **Close**.
A confirmation message is displayed in the **Guest Splash Administration** screen footer.

- 7 To import a guest file, do one of the following:
 - If you have Guest Splash Manager rights, log onto the controller.
 - If you have full administrator rights:
 - From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
 - In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
 - Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
 - In the **Guest Splash** section, click **Manage Guest Users**.
 - The **GuestPortal Guest Administration** screen displays.



	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		<input checked="" type="checkbox"/>
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		<input checked="" type="checkbox"/>

- 8 In the **File Management** section, click **Import Guest File**.
The **Import Guest File** dialog is displayed.
- 9 Click **Browse** to navigate to the location of the .csv guest file that you want to import, and then click **Open**.
- 10 Click **Import**.
The file is imported and a confirmation message is displayed in the **Import Guest File** dialog.
- 11 Click **Close**.

Viewing and Printing a GuestPortal Account Ticket

You can view and print a GuestPortal account ticket from the **GuestPortal Guest Administration** screen. A GuestPortal account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account.

The controller is shipped with a default template for the GuestPortal account ticket. The template is an html page that is augmented with system placeholders that display information about the user.

You can also upload a custom GuestPortal ticket template for the controller. To upload a custom GuestPortal ticket template you need full administrator access rights on the controller. The filename of a custom GuestPortal ticket template must be .html. For more information, see [Working with the Guest Portal Ticket Page](#) on page 645.

To View Print a GuestPortal Account Ticket:

1 Do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
 - From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
 - In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
 - Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
 - In the **GuestPortal** section, click **Manage Guest Users**.
 - The **GuestPortal Guest Administration** screen displays.

The screenshot shows the GuestPortal Guest Administration interface. At the top, there is a search bar with the text "Search" and "User Name:" followed by a text input field and a "Search" button. To the right of the search bar is a button labeled "Print Ticket for Selected Account". Below the search bar is a table with the following columns: User Name, User ID, Session Lifetime (hrs), Account Lifetime (days), Activation Date Time, Description, and Enabled. The table contains two rows of data. Below the table is a large empty area. At the bottom of the interface, there are three groups of buttons: "Account Management" (Add Guest Account, Edit Selected Accounts, Remove Selected Accounts), "Account Enable/Disable" (Enable Selected Accounts, Disable Selected Accounts), and "File Management" (Import Guest File, Export Guest File).

	User Name	User ID	Session Lifetime (hrs)	Account Lifetime (days)	Activation Date Time	Description	Enabled
<input type="checkbox"/>	mark	Guest-mark	0	30	2010-08-10 15:40:00		✓
<input type="checkbox"/>	mark	mark	1	30	2010-08-04 13:51:00		✓

- In the guest account list, select the checkbox next to the user name whose guest account ticket you want to print a ticket, and then click **Print Ticket for Selected Account**. The **GuestPortal** ticket is displayed.

- Click **Print**. The **Print** dialog is displayed.
- Click **Print**.



Note

The default GuestPortal ticket page uses placeholder tags. For more information, see [Default GuestPortal Ticket Page](#) on page 651.

Working with the Guest Portal Ticket Page

From the GuestPortal ticket page, you can activate a GuestPortal ticket page, upload a customized GuestPortal ticket page to the controller, and delete a customized GuestPortal ticket page.



Note

The default GuestPortal ticket page cannot be deleted.

To work with the GuestPortal account ticket page, you need full administrator rights. You can work with the guest account ticket page from the **Settings** screen. A guest account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account.

Related Links

- [Working with a Custom GuestPortal Ticket Page](#) on page 646
- [Activating a GuestPortal Ticket Page](#) on page 646
- [Uploading a Custom GuestPortal Ticket Page](#) on page 646
- [Deleting a Custom GuestPortal Ticket Page](#) on page 646
- [Example Ticket Page](#) on page 651

Working with a Custom GuestPortal Ticket Page

A customized GuestPortal ticket page can be uploaded to the controller. When designing your customized GuestPortal ticket page, be sure to use the guest account information placeholder tags that are depicted in the default GuestPortal ticket page. For more information, see [Default GuestPortal Ticket Page](#) on page 651.

Activating a GuestPortal Ticket Page

To Activate a GuestPortal Ticket Page:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
- 3 Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
- 4 In the **GuestPortal** section, click **Configure Ticket Page**. The **Ticket Settings** dialog is displayed.
- 5 In the **Active Template** list, click the GuestPortal ticket page you want to activate, and then click **Apply**.

This list includes all GuestPortal ticket pages that have been uploaded to the controller.

Uploading a Custom GuestPortal Ticket Page

To upload a custom GuestPortal ticket page:

- 1 On the **Ticket Settings** dialog, click **Browse**. The **Choose file** dialog is displayed.
- 2 Navigate to the .html GuestPortal ticket page file that you want to upload to the controller, and then click **Open**. The file name is displayed in the **Upload Template** box.
- 3 Click **Apply**. The file is uploaded to the controller.

The **Active Template** list includes all GuestPortal ticket pages that have been uploaded to the controller.

Deleting a Custom GuestPortal Ticket Page

To Delete a Custom GuestPortal Ticket Page:

- 1 On the **Ticket Settings** dialog, in the **Active Template** list, click the GuestPortal ticket page you want to delete, and then click **Delete**.
A dialog prompts you to confirm you want to delete the **GuestPortal** ticket page.
- 2 To delete the file, click **OK**, and then click **Apply**.

Configuring Guest Password Patterns

This feature makes it easier for system administrators to create password patterns that the Wireless Assistant will use to auto generate guest passwords. You can specify a predefined pattern or you can

create a customized pattern. You must have full administrative rights to generate password patterns. Select from the following password patterns:

- Completely Random Sequence
- Two Words
- Phone number
- Postal Code
- Custom Pattern

The generator offers three character sets: Latin (ASCII), Cyrillic, and Greek.

Related Links

[To Configure a Guest Password Pattern](#) on page 647

To Configure a Guest Password Pattern

To generate a password pattern:

- 1 From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
- 2 In the left pane, expand the **WLAN Services** pane, click the dedicated WLAN Service that provides the temporary guest network services. The **WLAN Services configuration** window for that service displays.
- 3 Click the **Auth & Acct** tab, and then click **Configure**. The Settings screen displays.

- 4 In the GuestPortal section, click **Configure Password Generator**. The Configure password generator screen displays.

To generate a custom password pattern:

- 1 From the Pattern pane, select **Custom**.
- 2 Select the character set and minimum password length.
- 3 Use the keypad to enter the pattern characters or type the pattern in the Pattern field.



Note

You can only type characters that are represented on the keypad. Entries in the **Pattern** field are editable.

The **Clear** key on the keypad clears the full pattern.

The **Clear Entry** key on the keypad clears the last entered character.

The password pattern displays in the **Pattern** field. Copy paste this pattern into the **Add Guest User** dialog. For more information, see [Adding New Guest Accounts](#) on page 635.

- 5 Click **Close** to close the dialog and save the password pattern.
- 6 Click **Cancel** to close the dialog without saving the password pattern.

Configuring Web Session Timeouts

You can configure the time period to allow web sessions to remain inactive before timing out. To configure web session timeouts:

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

The **Wireless Controller Configuration** screen displays.

- 2 In the left pane, click **Administration > Web Settings**

The **Wireless Controller Web Management Settings** screen displays.

The screenshot shows the 'Wireless Controller Web Management Settings' interface. At the top, there is a navigation bar with tabs for 'Logs', 'Reports', 'Controller' (which is selected and highlighted in purple), 'AP', 'VNS', and 'Radar'. Below this, the main content area has a header 'Wireless Controller Web Management Settings'. Underneath, there are two configuration fields. The first is 'Web Session Timeout' with a text input box containing '24:00' and a label '(hour:minutes, or just minutes)'. The second is 'GuestPortal Manager Web Session Timeout' with a text input box containing '1:00' and a label '(hour:minutes, or just minutes)'. Below these fields, there is a note: 'range 1 minute to 7 days'. In the bottom right corner, there is a 'Save' button.

- 3 In the **Web Session Timeout** box, type the time period to allow the web session to remain inactive before it times out.

This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.

- 4 In the **GuestPortal Manager Web Session Timeout** box, type the time period to allow the GuestPortal web session to remain inactive before it times out.

This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.

- 5 To save your settings, click **Save**.



Note

Screens that auto-refresh will time-out unless a manual action takes place prior to the end of the timeout period.

A Regulatory Information

ExtremeWireless APs 37XX , 38XX, and 39XX



Warning

Warnings identify essential information. Ignoring a warning can lead to problems with the application.



Note

For technical specifications and certification information for a specific Outdoor AP refer to the appropriate AP Installation Guide.

Configuration of the ExtremeWireless AP frequencies and power output are controlled by the regional software license and proper selection of the country during initial installation and set-up. Customers are allowed to select only the proper country from their licensed regulatory domain related to that customer's geographic location, performing the set-up of access points in accordance with local laws and regulations. The ExtremeWireless AP must not be operated until configured with the correct country setting or it may be in violation of the local laws and regulations.



Warning

Changes or modifications made to the APs which are not expressly approved by Extreme Networks could void the user's authority to operate the equipment. Only authorized Extreme Networks service personnel are permitted to service the system. Procedures that must be performed only by Extreme Networks personnel are clearly identified in the respective AP guide.



Note

The APs are in compliance with the European Directive 2002/95/EC on the restriction of the use of certain hazardous substances (RoHS) in electrical and electronic equipment.

ExtremeWireless APs 37XX , 38XX, and 39XX

For regulatory information for the ExtremeWireless AP models 37xx, 38xx, and 39XX refer to the appropriate AP *Installation Guide*.

B Default GuestPortal Ticket Page

Example Ticket Page

Example Ticket Page

PRINT

GuestPortal

Guest Name: test0001
User ID: test0001
Password: abcd1234
Account Start: 2009-10-22 12:53:00
Duration: 30 days
Valid Daily Login Time: 12:00AM -- 12:00AM
Comment:

System Requirements:

- A laptop with WLAN capabilities (801.11a/b/g). This functionality can be either embedded into your device or via a PCMCIA card.
- Web browser software. You can use any standard Internet browser (ie, Internet Explorer, Netscape, etc).

Instructions:

- Enable your wireless device to connect to the 'CNL-209-Guest' SSID.
- Once connected, launch your Internet browser and you will be redirected to the Guest Access webpage.
- Enter the user ID and password supplied above. By logging into the network, you are accepting the terms and conditions below.
- You're connected!

Placeholders Used in the Default GuestPortal Ticket Page

Table 123: Default GuestPortal Ticket Page Template Placeholders

Placeholder tag	Description
!GuestName	Guest Name
!GuestComment	Guest Comment
!TimeOfDayStart	Time-of-day start
!TimeOfDayDuration	Time-of-day session duration
!SessionLifeTime	Maximum session time
!UserID	User ID for the guest
!Password	Password for the guest
!SSID	SSID to connect to

Table 123: Default GuestPortal Ticket Page Template Placeholders (continued)

Placeholder tag	Description
!AccountActivationTime	Account available time
!AccountLifeTime	Account life time

Default GuestPortal Ticket Page Source Code



Note

The GuestPortal account information placeholders used in the html code are preceded by the ! character.

```
<HTML>
<HEAD>
    <title></title>
    <meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
</HEAD>
<body style="text-align:center">
    <table cellspacing="0" cellpadding="0" border="0" align="center" width="790">
    <tr>
        <td style="background-color:gray;color:white;font-weight:bold;font-size:
30;padding:5px"
align="center" width="790">GuestPortal</td>
    </tr>
    </table>
    <table cellspacing="5" cellpadding="0" border="0" style="margin:0 auto">
    <tr>
        <td align="right"><b>Guest Name:</b></td>
        <td align="left">!GuestName</td>
    </tr>
    <tr>
        <td align="right"><b>User ID:</b></td>
        <td align="left">!UserID</td>
    </tr>
    <tr>
        <td align="right"><b>Password:</b></td>
        <td align="left">!Password</td>
    </tr>
    <tr>
        <td align="right"><b>Account Start:</b></td>
        <td align="left">!AccountActivationTime</td>
    </tr>
    <tr>
        <td align="right"><b>Duration:</b></td>
        <td align="left">!AccountLifeTime</td>
    </tr>
    <tr>
        <td align="right"><b>Valid Daily Login Time:</b></td>
        <td align="left">!TimeOfDayStart -- !TimeOfDayDuration</td>
    </tr>
    <tr>
        <td align="right"><b>Comment:</b></td>
        <td align="left">!GuestComment</td>
    </tr>
    </table>
    <div style="width:790px;margin:0 auto;text-align:left">
        <b>System Requirements:</b>
        <hr width=790 size=2 noshade>
    </div>
</body>
</HTML>
```



```
<div style="padding-left:30px">
  <ul>
    <li>A laptop with WLAN capabilities (801.11a/b/g). This
functionality can be either embedded into your device or via a PCMCIA card.
    <li>Web browser software. You can use any standard
Internet browser (ie, Internet Explorer, Netscape, etc).
  </ul>
</div>
</div>
<div style="width:790px;margin:10px auto;text-align:left">
  <b>Instructions:</b>
  <hr width=790 size=2 noshade>
  <div style="padding-left:30px;">
    <ul>
      <li>Enable your wireless device to connect to the '!SSID'
SSID.
      <li>Once connected, launch your Internet browser and you
will be redirected to the Guest Access webpage.
      <li>Enter the user ID and password supplied above. By
logging into the network, you are accepting the terms and conditions below.
      <li>You're connected!
    </ul>
  </div>
</div>
</div>
</body>
</HTML>
```

C Glossary

A
B
C
D
E
F
G
H
I
J
L
M
N
O
P
Q
R
S
T
U
V
W
X

A

AAA

Authentication, authorization, and accounting. A system in IP-based networking to control which computer resources specific users can access and to keep track of the activity of specific users over the network.

ABR

Area border router. In [OSPF](#), an ABR has interfaces in multiple areas, and it is responsible for exchanging summary advertisements with other ABRs.

ACL

Access Control List. A mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP addresses, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

ACMI

Asynchronous Chassis Management Interface.

ad-hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP).

AES

Advanced Encryption Standard. AES is an algorithm for encryption that works at multiple network layers simultaneously. As a block cipher, AES encrypts data in fixed-size blocks of 128 bits; AES is also a privacy transform for IPSec and Internet Key Exchange (IKE). Created by the National Institute of Standards and Technology (NIST), the standard has a variable key length—it can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

For the WPA2/802.11i implementation of AES, a 128-bit key length is used. AES encryption includes four stages that make up one round. Each round is then iterated 10, 12, or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.

AES-CCMP

Advanced Encryption Standard - Counter-Mode/CBC-MAC Protocol. CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

alternate port

In **RSTP**, the alternate port supplies an alternate path to the root bridge and the root port.

AP (access point)

In wireless technology, access points are LAN transceivers or "base stations" that can connect to the regular wired network and forward and receive the radio signals that transmit wireless data.

area

In **OSPF**, an area is a logical set of segments connected by routers. The topology within an area is hidden from the rest of the **autonomous system (AS)**.

ARP

Address Resolution Protocol. ARP is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

AS

Autonomous system. In **OSPF**, an AS is a connected segment of a network topology that consists of a collection of subnetworks (with hosts attached) interconnected by a set of routes. The subnetworks and the routers are expected to be under the control of a single administration. Within an AS, routers may use one or more interior routing protocols and sometimes several sets of metrics. An AS is expected to present to other autonomous systems an appearance of a coherent interior routing plan and a

consistent picture of the destinations reachable through the AS. An AS is identified by a unique 16-bit number.

ASBR

Autonomous system border router. In **OSPF**, an ASBR acts as a gateway between OSPF and other routing protocols or other autonomous systems.

association

A connection between a wireless device and an access point.

asynchronous

See **ATM**.

ATM

Asynchronous transmission mode. A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

autobind

In **STP**, autobind (when enabled) automatically adds or removes ports from the STPD. If ports are added to the carrier VLAN, the member ports of the VLAN are automatically added to the STPD. If ports are removed from the carrier VLAN, those ports are also removed from the STPD.

autonegotiation

As set forth in IEEE 802.3u, autonegotiation allows each port on the switch—in partnership with its link partner—to select the highest speed between 10 Mbps and 100 Mbps and the best duplex mode.

B**backbone area**

In **OSPF**, a network that has more than one area must have a backbone area, configured as 0.0.0.0. All areas in an autonomous system (AS) must connect to the backbone area.

backup port

In **RSTP**, the backup port supports the designated port on the same attached LAN segment. Backup ports exist only when the bridge is connected as a self-loop or to a shared media segment.

backup router

In **VRRP**, the backup router is any VRRP router in the VRRP virtual router that is not elected as the master. The backup router is available to assume forwarding responsibility if the master becomes unavailable.

BDR

Backup designated router. In OSPF, the system elects a designated router (DR) and a BDR. The BDR smooths the transition to the DR, and each multi-access network has a BDR. The BDR is adjacent to all routers on the network and becomes the DR when the previous DR fails. The period of disruption in transit traffic lasts only as long as it takes to flood the new LSAs (which announce the new DR). The BDR is elected by the protocol; each hello packet has a field that specifies the BDR for the network.

BGP

Border Gateway Protocol. BGP is a router protocol in the IP suite designed to exchange network reachability information with BGP systems in other autonomous systems. You use a fully meshed configuration with BGP.

BGP provides routing updates that include a network number, a list of ASs that the routing information passed through, and a list of other path attributes. BGP works with cost metrics to choose the best available path; it sends updated router information only when one host has detected a change, and only the affected part of the routing table is sent.

BGP communicates within one AS using Interior BGP (IBGP) because BGP does not work well with IGP. Thus the routers inside the AS maintain two routing tables: one for the IGP and one for IBGP. BGP uses exterior BGP (EBGP) between different autonomous systems.

bi-directional rate shaping

A hardware-based technology that allows you to manage bandwidth on Layer 2 and Layer 3 traffic flowing to each port on the switch and to the backplane, per physical port on the I/O module. The parameters differ across platforms and modules.

blackhole

In the Extreme Networks implementation, you can configure the switch so that traffic is silently dropped. Although this traffic appears as received, it does not appear as transmitted (because it is dropped).

BOOTP

Bootstrap Protocol. BOOTP is an Internet protocol used by a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file that can be loaded into memory to boot the machine. Using BOOTP, a workstation can boot without a hard or floppy disk drive.

BPDU

Bridge protocol data unit. In **STP**, a BPDU is a packet that initiates communication between devices. BPDU packets contain information on ports, addresses, priorities, and costs and they ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

bridge

In conventional networking terms, bridging is a Layer 2 function that passes frames between two network segments; these segments have a common network layer address. The bridged frames pass only to those segments connected at a Layer 2 level, which is called a broadcast domain (or VLAN). You must use Layer 3 routing to pass frames between broadcast domains (VLANs).

In wireless technology, bridging refers to forwarding and receiving data between radio interfaces on APs or between clients on the same radio. So, bridged traffic can be forwarded from one AP to another AP without having to pass through the switch on the wired network.

broadcast

A broadcast message is forwarded to all devices within a VLAN, which is also known as a broadcast domain. The broadcast domain, or VLAN, exists at a Layer 2 level; you must use Layer 3 routing to

communicate between broadcast domains, or VLANs. Thus, broadcast messages do not leave the VLAN. Broadcast messages are identified by a broadcast address.

BSS

Basic Service Set. A wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also IBSS.

C

captive portal

A browser-based authentication mechanism that forces unauthenticated users to a web page.

carrier VLAN

In **STP**, carrier VLANs define the scope of the STPD, including the physical and logical ports that belong to the STPD as well as the 802.1Q tags used to transport EMISTP- or PVST+-encapsulated BPDUs. Only one carrier VLAN can exist in any given STPD.

CCM

In **CFM**, connectivity check messages are CFM frames transmitted periodically by a MEP to ensure connectivity across the maintenance entities to which the transmitting MEP belongs. The CCM messages contain a unique ID for the specified domain. Because a failure to receive a CCM indicates a connectivity fault in the network, CCMs proactively check for network connectivity.

CDR

Call Data (Detail) Record

. In Internet telephony, a call detail record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call.

In essence, call accounting is a database application that processes call data from your switch (PBX, iPBX, or key system) via a CDR (call detail record) or SMDR (station message detail record) port. The call data record details your system's incoming and outgoing calls by thresholds, including time of call, duration of call, dialing extension, and number dialed. Call data is stored in a PC database.

CEP

Customer Edge Port. Also known as Selective Q-in-Q or C-tagged Service Interface. CEP is a role that is configured in software as a CEP VMAN port, and connects a VMAN to specific CVLANs based on the CVLAN CVID. The CNP role, which is configured as an untagged VMAN port, connects a VMAN to all other port traffic that is not already mapped to the port CEP role.

CA certificate

A certificate identifying a certificate authority. A CA certificate can be used to verify that a certificate issued by the certificate authority is legitimate.

certificate

A document that identifies a server or a client (user), containing a public key and signed by a certificate authority.

Certificate Authority (CA)

A trusted third-party that generates and signs certificates. A CA may be a commercial concern, such as GoDaddy or GeoTrust. A CA may also be an in-house server for certificates used within an enterprise.

certificate chain

An ordered set of certificates which can be used to verify the identity of a server or client. It begins with a client or server certificate, and ends with a certificate that is trusted.

certificate issuer

The certificate authority that generated the certificate.

Certificate Signing Request (CSR)

A document containing identifiers, options, and a public key, that is sent to a certificate authority in order to generate a certificate.

certificate subject

The server or client identified by the certificate.

client certificate

A certificate identifying a client (user). A client certificate can be used in conjunction with, or in lieu of, a username and password to authenticate a client.

CFM

Connectivity Fault Management allows an ISP to proactively detect faults in the network for each customer service instance individually and separately. CFM comprises capabilities for detecting, verifying, and isolating connectivity failures in virtual bridged LANs.

Chalet

A web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure than because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

checkpointing

Checkpointing is the process of copying the active state configurations from the primary MSM to the backup MSM on modular switches.

CIDR

Classless Inter-Domain Routing. CIDR is a way to allocate and specify the Internet addresses used in interdomain routing more flexibly than with the original system of IP address classes. This address aggregation scheme uses supernet addresses to represent multiple IP destinations. Rather than advertise a separate route for each destination, a router uses a supernet address to advertise a single route representing all destinations. RIP does not support CIDR; BGP and OSPF support CIDR.

CIST

Common and Internal Spanning Tree. In an **MSTP** environment, the CIST is a single spanning tree domain that connects MSTP regions. The CIST is responsible for creating a loop-free topology by exchanging and propagating BPDUs across MSTP regions. You can configure only one CIST on each switch.

CIST regional root bridge

Within an **MSTP** region, the bridge with the lowest path cost to the CIST root bridge is the CIST regional root bridge. If the CIST root bridge is inside an MSTP region, that same bridge is the CIST regional root for that region because it has the lowest path cost to the CIST root. If the CIST root bridge is outside an MSTP region, all regions connect to the CIST root through their respective CIST regional roots.

CIST root bridge

In an **MSTP** environment, the bridge with the lowest bridge ID becomes the CIST root bridge. The bridge ID includes the bridge priority and the MAC address. The CIST root bridge can be either inside or outside an MSTP region. The CIST root bridge is unique for all regions and non-MSTP bridges, regardless of its location.

CIST root port

In an **MSTP** environment, the port on the CIST regional root bridge that connects to the CIST root bridge is the CIST root port. The CIST root port is the master port for all MSTIs in that MSTP region, and it is the only port that connects the entire region to the CIST root bridge.

CLEAR-flow

CLEAR-Flow allows you to specify certain types of traffic to perform configured actions on. You can configure the switch to take an immediate, preconfigured action to the specified traffic or to send a copy of the traffic to a management station for analysis. CLEAR-Flow is an extension to **ACLs**, so you must be familiar with ACL policy files to apply CLEAR-Flow.

CLI

Command Line Interface. You can use the CLI to monitor and manage the switch or wireless appliance.

cluster

In **BGP**, a cluster is formed within an **AS** by a route reflector and its client routers.

collision

Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.

CNA

Converged Network Analyzer. This application suite, available from Avaya, allows the server to determine the best possible network path. The CNA Agent is a software piece of the entire CNA application that you install on Extreme Networks devices. You use the CNA Agent software only if you are using the Avaya CNA solution, and the CNA Agent cannot function unless you also obtain the rest of the CNA application from Avaya.

CNP

Customer Network Port.

combo port

Also known as a combination port. On some Extreme Networks devices (such as the X440-G2 series switch), certain ports can be used as either copper or fibre ports.

combo link

In [EAPS](#), the common link is the physical link between the controller and partner nodes in a network where multiple EAPS share a common link between domains.

control VLAN

In [EAPS](#), the control VLAN is a VLAN that sends and receives EAPS messages. You must configure one control VLAN for each EAPS domain.

controller node

In [EAPS](#), the controller node is that end of the common line that is responsible for blocking ports if the common link fails, thereby preventing a superloop.

CoS

Class of Service. Specifying the service level for the classified traffic type. For more information, see QoS in the [ExtremeXOS 21.1 User Guide](#).

CRC

Cyclic Redundancy Check. This simple checksum is designed to detect transmission errors. A decoder calculates the CRC for the received data and compares it to the CRC that the encoder calculated, which is appended to the data. A mismatch indicates that the data was corrupted in transit.

CRC error

Cyclic redundancy check error. This is an error condition in which the data failed a checksum test used to trap transmission errors. These errors can indicate problems anywhere in the transmission path.

CSPF

Constrained shortest path first. An algorithm based on the shortest path first algorithm used in [OSPF](#), but with the addition of multiple constraints arising from the network, the LSP, and the links. CSPF is used to minimize network congestion by intelligently balancing traffic.

CVID

CVLAN ID. The CVID represents the CVLAN tag for tagged VLAN traffic. (See [CVLAN](#).)

CVLAN

Customer VLAN.

D**DAD**

Duplicate Address Detection. IPv6 automatically uses this process to ensure that no duplicate IP addresses exist. For more information, see Duplicate Address Detection in the [ExtremeXOS 21.1 User Guide](#).

dBm

An abbreviation for the power ratio in decibels (dB) of the measured power referenced to one milliwatt.

DCB

is a set of IEEE 802.1Q extensions to standard Ethernet, that provide an operational framework for unifying Local Area Networks (LAN), Storage Area Networks (SAN) and Inter-Process Communication (IPC) traffic between switches and endpoints onto a single transport layer.

DCBX

The Data Center Bridging eXchange protocol is used by DCB devices to exchange DCB configuration information with directly connected peers.

default encapsulation mode

In **STP**, default encapsulation allows you to specify the type of BPDU encapsulation to use for all ports added to a given STPD, not just to one individual port. The encapsulation modes are:

- 802.1d—This mode is used for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1d.
- EMISTP—Extreme Multiple Instance Spanning Tree Protocol (EMISTP) mode is an extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs.
- PVST+—This mode implements PVST+ in compatibility with third-party switches running this version of STP.

designated port

In **STP**, the designated port provides the shortest path connection to the root bridge for the attached LAN segment. Each LAN segment has only one designated port.

destination address

The IP or MAC address of the device that is to receive the packet.

Device Manager

The Device Manager is an Extreme Networks-proprietary process that runs on every node and is responsible for monitoring and controlling all of the devices in the system. The Device Manager is useful for system redundancy.

device server

A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers, and network time servers are examples of device servers.

DF

Don't fragment bit. This is the don't fragment bit carried in the flags field of the IP header that indicates that the packet should not be fragmented. The remote host will return ICMP notifications if the packet had to be split anyway, and these are used in **MTU** discovery.

DHCP

Dynamic Host Configuration Protocol. DHCP allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DiffServ

Differentiated Services. Defined in RFC 2474 and 2475, DiffServ is an architecture for implementing scalable service differentiation in the Internet. Each IP header has a DiffServ (DS) field, formerly known as the Type of Service (TOS) field. The value in this field defines the QoS priority the packet will have throughout the network by dictating the forwarding treatment given to the packet at each node.

DiffServ is a flexible architecture that allows for either end-to-end QoS or intra-domain QoS by implementing complex classification and mapping functions at the network boundary or access points. In the Extreme Networks implementation, you can configure the desired QoS by replacing or mapping the values in the DS field to egress queues that are assigned varying priorities and bandwidths.

directory agent (DA)

A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices. With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'.

The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.

For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.

(SLP version 2, RFC 2608, updating RFC 2165)

diversity antenna and receiver

The AP has two antennae. Receive diversity refers to the ability of the AP to provide better service to a device by receiving from the user on which ever of the two antennae is receiving the cleanest signal. Transmit diversity refers to the ability of the AP to use its two antenna to transmit on a specific antenna only, or on a alternate antennae. The antennae are called diversity antennae because of this capability of the pair.

DNS

Domain Name Server. This system is used to translate domain names to IP addresses. Although the Internet is based on IP addresses, names are easier to remember and work with. All these names must be translated back to the actual IP address and the DNS servers do so.

domain

In CFM, a maintenance domain is the network, or part of the network, that belongs to a single administration for which connectivity faults are managed.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks. For more information, see DoS Protection in the *ExtremeXOS 21.1 User Guide*.

DR

Designated router. In OSPF, the DR generates an LSA for the multi-access network and has other special responsibilities in the running of the protocol. The DR is elected by the OSPF protocol.

DSSS

Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with [FHSS](#).)

DTIM

DTIM delivery traffic indication message (in 802.11 standard).

dynamic WEP

The IEEE introduced the concept of user-based authentication using per-user encryption keys to solve the scalability issues that surrounded static WEP. This resulted in the 802.1x standard, which makes use of the IETF's Extensible Authentication Protocol (EAP), which was originally designed for user authentication in dial-up networks. The 802.1x standard supplemented the EAP protocol with a mechanism to send an encryption key to a Wireless AP. These encryption keys are used as dynamic WEP keys, allowing traffic to each individual user to be encrypted using a separate key.

E**EAPS**

Extreme Automatic Protection Switching. This is an Extreme Networks-proprietary version of the Ethernet Automatic Protection Switching protocol that prevents looping Layer 2 of the network. This feature is discussed in RFC 3619.

EAPS domain

An EAPS domain consists of a series of switches, or nodes, that comprise a single ring in a network. An EAPS domain consists of a master node and transit nodes. The master node consists of one primary and one secondary port. EAPS operates by declaring an EAPS domain on a single ring.

EAPS link ID

Each common link in the EAPS network must have a unique link ID. The controller and partner shared ports belonging to the same common link must have matching link IDs, and not other instance in the network should have that link ID.

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically

generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

(See also [PEAP](#).)

EBGP

Exterior Border Gateway Protocol. EBGP is a protocol in the IP suite designed to exchange network reachability information with BGP systems in other [autonomous systems](#). EBGP works between different ASs.

ECMP

Equal Cost Multi Paths. This routing algorithm distributes network traffic across multiple high-bandwidth [OSPF](#), [BGP](#), IS-IS, and static routes to increase performance. The Extreme Networks implementation supports multiple equal cost paths between points and divides traffic evenly among the available paths.

edge ports

In [STP](#), edge ports connect to non-STP devices such as routers, endstations, and other hosts.

edge safeguard

Loop prevention and detection on an edge port configured for [RSTP](#) is called [edge safeguard](#). Configuring edge safeguard on RSTP edge ports can prevent accidental or deliberate misconfigurations (loops) resulting from connecting two edge ports together or from connecting a hub or other non-STP switch to an edge port. Edge safeguard also limits the impact of broadcast storms that might occur on edge ports. This advanced loop prevention mechanism improves network resiliency but does not interfere with the rapid convergence of edge ports. For more information about edge safeguard, see [Configuring Edge Safeguard](#) in the *ExtremeXOS 21.1 User Guide*.

EDP

Extreme Discovery Protocol. EDP is a protocol used to gather information about neighbor Extreme Networks switches. Extreme Networks switches use EDP to exchange topology information.

EEPROM

Electrically erasable programmable read-only memory. EEPROM is a memory that can be electronically programmed and erased but does not require a power source to retain data.

EGP

Exterior Gateway Protocol. EGP is an Internet routing protocol for exchanging reachability information between routers in different [autonomous systems](#). [BGP](#) is a more recent protocol that accomplishes this task.

election algorithm

In [ESRP](#), this is a user-defined criteria to determine how the master and slave interact. The election algorithm also determines which device becomes the master or slave and how [ESRP](#) makes those decisions.

ELRP

Extreme Loop Recovery Protocol. ELRP is an Extreme Networks-proprietary protocol that allows you to detect Layer 2 loops.

ELSM

Extreme Link Status Monitoring. ELSM is an Extreme Networks-proprietary protocol that monitors network health. You can also use ELSM with Layer 2 control protocols to improve Layer 2 loop recovery in the network.

EMISTP

Extreme Multiple Instance Spanning Tree Protocol. This Extreme Networks-proprietary protocol uses a unique encapsulation method for STP messages that allows a physical port to belong to multiple STPDs.

EMS

Event Management System. This Extreme Networks-proprietary system saves, displays, and filters events, which are defined as any occurrences on a switch that generate a log message or require action.

encapsulation mode

Using [STP](#), you can configure ports within an STPD to accept specific BPDU encapsulations. The three encapsulation modes are:

- 802.1D—This mode is used for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1D.
- EMISTP—Extreme Multiple Instance Spanning Tree Protocol mode is an extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs.
- PVST+—This mode implements PVST+ in compatibility with third-party switches running this version of STP.

EPICenter

See [Ridgeline](#).

ESRP

Extreme Standby Router Protocol. ESRP is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

ESRP-aware device

This is an Extreme Networks device that is not running ESRP itself but that is connected on a network with other Extreme Networks switches that are running ESRP. These ESRP-aware devices also fail over.

ESRP domain

An ESRP domain allows multiple VLANs to be protected under a single logical entity. An ESRP domain consists of one domain-master VLAN and zero or more domain-member VLANs.

ESRP-enabled device

An ESRP-enabled device is an Extreme Networks switch with an ESRP domain and ESRP enabled. ESRP-enabled switches include the ESRP master and slave switches.

ESRP extended mode

ESRP extended mode supports and is compatible only with switches running ExtremeXOS software exclusively.

ESRP group

An ESRP group runs multiple instances of ESRP within the same VLAN (or broadcast domain). To provide redundancy at each tier, use a pair of ESRP switches on the group.

ESRP instance

You enable ESRP on a per domain basis; each time you enable ESRP is an ESRP instance.

ESRP VLAN

A VLAN that is part of an ESRP domain, with ESRP enabled, is an ESRP VLAN.

ESS

Extended Service Set. Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. (See [BSS](#) and [SSID](#).)

ethernet

This is the IEEE 802.3 networking standard that uses carrier sense multiple access with collision detection (CSMA/CD). An Ethernet device that wants to transmit first checks the channel for a carrier, and if no carrier is sensed within a period of time, the device transmits. If two devices transmit simultaneously, a collision occurs. This collision is detected by all transmitting devices, which subsequently delay their retransmissions for a random period. Ethernet runs at speeds from 10 Mbps to 10 Gbps on full duplex.

event

Any type of occurrence on a switch that could generate a log message or require an action. For more, see [syslog](#).

external table

To route traffic between [autonomous systems](#), external routing protocols and tables, such as [EGP](#) and [BGP](#), are used.

F**fabric module (FM)**

For more information about available fabric modules, see "Fabric Modules" in the [ExtremeSwitching X8 Series Switches Hardware Installation Guide](#).

fast convergence

In [EAPS](#), Fast Convergence allows convergence in the range of 50 milliseconds. This parameter is configured for the entire switch, not by EAPS domain.

fast path

This term refers to the data path for a packet that traverses the switch and does not require processing by the CPU. Fast path packets are handled entirely by ASICs and are forwarded at wire speed rate.

FDB

Forwarding database. The switch maintains a database of all MAC address received on all of its ports and uses this information to decide whether a frame should be forwarded or filtered. Each FDB entry consists of the MAC address of the sending device, an identifier for the port on which the frame was

received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not currently in the FDB are flooded to all members of the VLAN. For some types of entries, you configure the time it takes for the specific entry to age out of the FDB.

FHSS

Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with [DSSS](#).)

FIB

Forwarding Information Base. On BlackDiamond 8800 series switches and Summit family switches, the Layer 3 routing table is referred to as the FIB.

fit, thin, and fat APs

A *thin* AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required.

A *fit* AP, a variation of the thin AP, handles the RF and encryption, while the central management controller, aware of the wireless users' identities and locations, handles secure roaming, quality of service, and user authentication. The central management controller also handles AP configuration and management.

A *fat* (or thick) AP architecture concentrates all the WLAN intelligence in the access point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.

frame

This is the unit of transmission at the data link layer. The frame contains the header and trailer information required by the physical medium of transmission.

FQDN

Fully Qualified Domain Name. A 'friendly' designation of a computer, of the general form computer.[subnetwork.]organization.domain. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a [DNS](#).

full-duplex

This is the communication mode in which a device simultaneously sends and receives over the same link, doubling the bandwidth. Thus, a full-duplex 100 Mbps connection has a bandwidth of 200 Mbps, and so forth. A device either automatically adjusts its duplex mode to match that of a connecting device or you can configure the duplex mode; all devices at 1 Gbps or higher run only in full-duplex mode.

FTM

Forwarding Table Manager.

FTP

File Transfer Protocol.

G

gateway

In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

gigabit ethernet

This is the networking standard for transmitting data at 1000 Mbps or 1 Gbps. Devices can transmit at multiples of gigabit Ethernet as well.

gratuitous ARP

When a host sends an ARP request to resolve its own IP address, it is called gratuitous ARP. For more information, see Gratuitous ARP Protection in the *ExtremeXOS 21.1 User Guide*.

GUI

Graphical User Interface.

H

HA

Host Attach. In ExtremeXOS software, HA is part of ESRP that allows you to connect active hosts directly to an ESRP switch; it allows configured ports to continue Layer 2 forwarding regardless of their ESRP status.

half-duplex

This is the communication mode in which a device can either send or receive data, but not simultaneously. (Devices at 1 Gbps or higher do not run in half-duplex mode; they run only in full-duplex mode.)

header

This is control information (such as originating and destination stations, priority, error checking, and so forth) added in front of the data when encapsulating the data for network transmission.

heartbeat message

A UDP data packet used to monitor a data connection, polling to see if the connection is still alive. In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.

hitless failover

In the Extreme Networks implementation on modular switches and SummitStacks, hitless failover means that designated configurations survive a change of primacy between the two MSMs (modular switches) or master/backup nodes (SummitStacks) with all details intact. Thus, those features run seamlessly during and after control of the system changes from one MSM or node to another.

host

- 1 A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines.

- 2 A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

HTTP

Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1)

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

IBGP

Interior Border Gateway Protocol. IBGP is the **BGP** version used within an **AS**.

IBSS

Independent Basic Service Set (see **BSS**). An IBSS is the 802.11 term for an ad-hoc network. See **ad-hoc mode**.

ICMP

Internet Control Message Protocol. ICMP is the part of the TCP/IP protocol that allows generation of error messages, test packets, and operating messages. For example, the ping command allows you to send ICMP echo messages to a remote IP device to test for connectivity. ICMP also supports traceroute, which identifies intermediate hops between a given source and destination.

ICV

ICV (Integrity Check Value) is a 4-byte code appended in standard **WEP** to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (See **WPA** and **MIC**.)

IEEE

Institute of Electrical and Electronic Engineers. This technical professional society fosters the development of standards that often become national and international standards. The organization publishes a number of journals and has many local chapters and several large societies in special areas.

IETF

Internet Engineering Task Force. The IETF is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The technical work of the IETF is done in working groups, which are organized by topic.

IGMP

Internet Group Management Protocol. Hosts use IGMP to inform local routers of their membership in multicast groups. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. When all hosts leave a group, the router no longer forwards packets that arrive for the multicast group.

IGMP snooping

This provides a method for intelligently forwarding multicast packets within a Layer 2 broadcast domain. By “snooping” the IGMP registration information, the device forms a distribution list that determines which endstations receive packets with a specific multicast address. Layer 2 switches listen for IGMP messages and build mapping tables and associated forwarding filters. IGMP snooping also reduces IGMP protocol traffic.

IGP

Interior Gateway Protocol. IGP refers to any protocol used to exchange routing information within an AS. Examples of Internet IGPs include [RIP](#) and [OSPF](#).

inline power

According to IEEE 802.3 af, inline power refers to providing an AC or DC power source through the same cable as the data travels. It allows phones and network devices to be placed in locations that are not near AC outlets. Most standard telephones use inline power.

infrastructure mode

An 802.11 networking framework in which devices communicate with each other by first going through an access point. In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (See [ad-hoc mode](#) and [BSS](#).)

intermediate certificate

A certificate in the middle of a certificate chain, that bridges the trust relationship between the server certificate and the trusted certificate.

IP

Internet Protocol. The communications protocol underlying the Internet, IP allows large, geographically diverse networks of computers to communicate with each other quickly and economically over a variety of physical links; it is part of the TCP/IP suite of protocols. IP is the Layer 3, or network layer, protocol that contains addressing and control information that allows packets to be routed. IP is the most widely used networking protocol; it supports the idea of unique addresses for each computer on the network. IP is a connectionless, best-effort protocol; TCP reassembles the data after transmission. IP specifies the format and addressing scheme for each packet.

IPC

Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.

IPsec/IPsec-ESP/IPsec-AH

Internet Protocol security (IPSec)

Internet Protocol security.

Encapsulating Security Payload (IPsec-ESP)

The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram.

**Internet Protocol security
Authentication Header (IPsec-AH)**

AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver.

IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

IPv6

Internet Protocol version 6. IPv6 is the next-generation IP protocol. The specification was completed in 1997 by IETF. IPv6 is backward-compatible with and is designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited (for all intents and purposes) number of networks and systems; IPv6 is expected to slowly replace IPv4, with the two existing side by side for many years.

IP address

IP address is a 32-bit number that identifies each unique sender or receiver of information that is sent in packets; it is written as four octets separated by periods (dotted-decimal format). An IP address has two parts: the identifier of a particular network and an identifier of the particular device (which can be a server or a workstation) within that network. You may add an optional sub-network identifier. Only the network part of the address is looked at between the routers that move packets from one point to another along the network. Although you can have a static IP address, many IP addresses are assigned dynamically from a pool. Many corporate networks and online services economize on the number of IP addresses they use by sharing a pool of IP addresses among a large number of users. (The format of the IP address is slightly changed in IPv6.)

IPTV

Internal Protocol television. IPTV uses a digital signal sent via broadband through a switched telephone or cable system. An accompanying set top box (that sits on top of the TV) decodes the video and converts it to standard television signals.

IR

Internal router. In [OSPF](#), IR is an internal router that has all interfaces within the same area.

IRDP

Internet Router Discovery Protocol. Used with IP, IRDP enables a host to determine the address of a router that it can use as a default gateway. In Extreme Networks implementation, IP multinetting requires a few changes for the IRDP.

ISO

This abbreviation is commonly used for the International Organization for Standardization, although it is not an acronym. ISO was founded in 1946 and consists of standards bodies from more than 75 nations.

ISO had defined a number of important computer standards, including the OSI reference model used as a standard architecture for networking.

isochronous

Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.

ISP

An Internet Service Provider is an organization that provides access to the Internet. Small ISPs provide service via modem and ISDN while the larger ones also offer private line hookups (T1, fractional T1, etc.). Customers are generally billed a fixed rate per month, but other charges may apply. For a fee, a Web site can be created and maintained on the ISP's server, allowing the smaller organization to have a presence on the Web with its own domain name.

ITU-T

International Telecommunication Union-Telecommunication. The ITU-T is the telecommunications division of the ITU international standards body.

IV

Initialization Vector. Part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases the difficulty in cracking the encryption. (See [WPA](#) and [TKIP](#).)

J**jumbo frames**

Ethernet frames larger than 1522 bytes (including the 4 bytes in the [CRC](#)). The jumbo frame size is configurable on Extreme Networks devices; the range is from 1523 to 9216 bytes.

L**LACP**

Link Aggregation Control Protocol. LACP is part of the IEEE 802.3ad and automatically configures multiple aggregated links between switches.

LAG

Link aggregation group. A LAG is the logical high-bandwidth link that results from grouping multiple network links in link aggregation (or load sharing). You can configure static LAGs or dynamic LAGs (using the LACP).

Layer 2

Layer 2 is the second, or data link, layer of the OSI model, or the MAC layer. This layer is responsible for transmitting frames across the physical link by reading the hardware, or MAC, source and destination addresses.

Layer 3

Layer 3 is the third layer of the OSI model. Also known as the network layer, Layer 3 is responsible for routing packets to different LANs by reading the network address.

LED

Light-emitting diode. LEDs are on the device and provide information on various states of the device's operation. See your hardware documentation for a complete explanation of the LEDs on devices running ExtremeXOS.

legacy certificate

The certificates that shipped with Extreme Management Center and NAC 4.0.0 and earlier.

LFS

Link Fault Signal. LFS, which conforms to IEEE standard 802.3ae-2002, monitors 10 Gbps ports and indicates either remote faults or local faults.

license

ExtremeXOS version 11.1 introduces a licensing feature to the ExtremeXOS software. You must have a license, which you obtain from Extreme Networks, to apply the full functionality of some features.

link aggregation

Link aggregation, also known as trunking or load sharing, conforms to IEEE 802.3ad. This feature is the grouping of multiple network links into one logical high-bandwidth link.

link type

In [OSPF](#), there are four link types that you can configure: auto, broadcast, point-to-point, and passive.

LLDP

Link Layer Discovery Protocol. LLDP conforms to IEEE 802.1ab and is a neighbor discovery protocol. Each LLDP-enabled device transmits information to its neighbors, including chassis and port identification, system name and description, VLAN names, and other selected networking information. The protocol also specifies timing intervals in order to ensure current information is being transmitted and received.

load sharing

Load sharing, also known as trunking or link aggregation, conforms to IEEE 802.3ad. This feature is the grouping of multiple network links into one logical high-bandwidth link. For example, by grouping four 100 Mbps of full-duplex bandwidth into one logical link, you can create up to 800 Mbps of bandwidth. Thus, you increase bandwidth and availability by using a group of ports to carry traffic in parallel between switches.

loop detection

In [ELRP](#), loop detection is the process used to detect a loop in the network. The switch sending the ELRP PDU waits to receive its original PDU back. If the switch received this original PDU, there is a loop in the network.

LSA

Link state advertisement. An LSA is a broadcast packet used by link state protocols, such as [OSPF](#). The LSA contains information about neighbors and path costs and is used by the receiving router to maintain a routing table.

LSDB

Link state database. In [OSPF](#), LSDB is a database of information about the link state of the network. Two neighboring routers consider themselves to be adjacent only if their LSDBs are synchronized. All routing information is exchanged only between adjacent routers.

M

MAC

Media Access Control layer. One of two sub-layers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one [NIC](#) to another across a shared channel.

MAC address

Media access control address. The MAC address, sometimes known as the hardware address, is the unique physical address of each network interface card on each device.

MAN

Metropolitan area network. A MAN is a data network designed for a town or city. MANs may be operated by one organization such as a corporation with several offices in one city, or be shared resources used by several organizations with several locations in the same city. MANs are usually characterized by very high-speed connections.

master node

In [EAPS](#), the master node is a switch, or node, that is designated the master in an EAPS domain ring. The master node blocks the secondary port for all non-control traffic belonging to this EAPS domain, thereby avoiding a loop in the ring.

master router

In [VRRP](#), the master router is the physical device (router) in the VRRP virtual router that is responsible for forwarding packets sent to the VRRP virtual router and for responding to ARP requests. The master router sends out periodic advertisements that let backup routers on the network know that it is alive. If the VRRP IP address owner is identified, it always becomes the master router.

master VLAN

In [ESRP](#), the master VLAN is the VLAN on the ESRP domain that exchanges ESRP-PDUs and data between a pair of ESRP-enabled devices. You must configure one master VLAN for each ESRP domain, and a master VLAN can belong to only one ESRP domain.

MED

Multiple exit discriminator. [BGP](#) uses the MED metric to select a particular border router in another AS when multiple border routers exist.

member VLAN

In [ESRP](#), you configure zero or more member VLANs for each ESRP domain. A member VLAN can belong to only one ESRP domain. The state of the ESRP device determines whether the member VLAN is in forwarding or blocking state.

MEP

In [CFM](#), maintenance end point is an end point for a single domain, or maintenance association. The MEP may be either an UP MEP or a DOWN MEP.

metering

In [QoS](#), metering monitors the traffic pattern of each flow against the traffic profile. For out-of-profile traffic the metering function interacts with other components to either re-mark or drop the traffic for that flow. In the Extreme Networks implementation, you use [ACLs](#) to enforce metering.

MIB

Management Information Base. MIBs make up a database of information (for example, traffic statistics and port settings) that the switch makes available to network management systems. MIB names identify objects that can be managed in a network and contain information about the objects. MIBs provide a means to configure a network device and obtain network statistics gathered by the device. Standard, minimal MIBs have been defined, and vendors often have private enterprise MIBs.

MIC

Message Integrity Check or Code (MIC), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.

Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (See [WPA](#), [TKIP](#), and [ICV](#).)

MIP

In [CFM](#), the maintenance intermediate point is intermediate between endpoints. Each MIP is associated with a single domain, and there may be more than one MIP in a single domain.

mirroring

Port mirroring configures the switch to copy all traffic associated with one or more ports to a designated monitor port. The monitor port can be connected to a network analyzer or RMON probe for packet analyzer.

MLAG

Multi-switch Link Aggregation Group (a.k.a. Multi-Chassis Link Aggregation Group). This feature allows users to combine ports on two switches to form a single logical connection to another network device. The other network device can be either a server or a switch that is separately configured with a regular LAG (or appropriate server port teaming) to form the port aggregation.

MM

Management Module. For more information, see "Management Modules" in the [ExtremeSwitching X8 Series Switches Hardware Installation Guide](#).

MMF

Multimode fiber. MMF is a fiber optic cable with a diameter larger than the optical wavelength, in which more than one bound mode can propagate. Capable of sending multiple transmissions simultaneously, MMF is commonly used for communications of 2 km or less.

MSDP

Multicast Source Discovery Protocol. MSDP is used to connect multiple multicast routing domains. MSDP advertises multicast sources across Protocol Independent Multicast-Sparse Mode (PIM-SM) multicast domains or Rendezvous Points (RPs). In turn, these RPs run MSDP over TCP to discover multicast sources in other domains.

MSM

Master Switch Fabric Module. This Extreme Networks-proprietary name refers to the module that holds both the control plane and the switch fabric for switches that run the ExtremeXOS software on modular switches. One MSM is required for switch operation; adding an additional MSM increases reliability and throughput. Each MSM has two CPUs. The MSM has LEDs as well as a console port, management port, modem port, and compact flash; it may have data ports as well. The MSM is responsible for upper-layer protocol processing and system management functions. When you save the switch configuration, it is saved to all MSMs.

MSTI

Multiple Spanning Tree Instances. MSTIs control the topology inside an MSTP region. An MSTI is a spanning tree domain that operates within a region and is bounded by that region; and MSTI does not exchange BPDUs or send notifications to other regions. You can map multiple VLANs to an MSTI; however, each VLAN can belong to only one MSTI. You can configure up to 64 MSTIs in an MSTP region.

MSTI regional root bridge

In an MSTP environment, each MSTI independently elects its own root bridge. The bridge with the lowest bridge ID becomes the MSTI regional root bridge. The bridge ID includes the bridge priority and the MAC address.

MSTI root port

In an MSTP environment, the port on the bridge with the lowest path cost to the MSTI regional root bridge is the MSTI root port.

MSTP

Multiple Spanning Tree Protocol. MSTP, based on IEEE 802.1Q-2003 (formerly known as IEEE 892.1s), allows you to bundle multiple VLANs into one spanning tree (STP) topology, which also provides enhanced loop protection and better scaling. MSTP uses RSTP as the converging algorithm and is compatible with legacy STP protocols.

MSTP region

An MSTP region defines the logical boundary of the network. Interconnected bridges that have the same MSTP configuration are referred to as an MSTP region. Each MSTP region has a unique identifier, is bound together by one CIST that spans the entire network, and contains from 0 to 64 MSTIs. A bridge participates in only one MSTP region at one time. An MSTP topology is individual MSTP regions connected either to the rest of the network with 802.1D and 802.1w bridges or to each other.

MTU

Maximum transmission unit. This term is a configurable parameter that determines the largest packet than can be transmitted by an IP interface (without the packet needing to be broken down into smaller units).

**Note**

Packets that are larger than the configured MTU size are dropped at the ingress port. Or, if configured to do so, the system can fragment the IPv4 packets and reassemble them at the receiving end.

multicast

Multicast messages are transmitted to selected devices that specifically join the multicast group; the addresses are specified in the destination address field. In other words, multicast (point-to-multipoint) is a communication pattern in which a source host sends a message to a group of destination hosts.

multinetting

IP multinetting assigns multiple logical IP interfaces on the same circuit or physical interface. This allows one bridge domain (VLAN) to have multiple IP networks.

MVR

Multicast VLAN registration. MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN; it allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the The application from the subscriber VLANs for bandwidth and security reasons. MVR allows a multicast stream received over a Layer 2 VLAN to be forwarded to another VLAN, eliminating the need for a Layer 3 routing protocol; this feature is often used for IPTV applications.

N**NAS**

Network Access Server. This is server responsible for passing information to designated **RADIUS** servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC 2138)

NAT

Network Address Translation (or Translator). This is a network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates a new IP address for each client computer on the network.

netlogin

Network login provides extra security to the network by assigning addresses only to those users who are properly authenticated. You can use web-based, MAC-based, or IEEE 802.1X-based authentication with network login. The two modes of operation are campus mode and ISP mode.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

neutral state/switch

In **ESRP**, the neutral state is the initial state entered by the switch. In a neutral state, the switch waits for ESRP to initialize and run. A neutral switch does not participate in ESRP elections.

NIC

Network Interface Card. An expansion board in a computer that connects the computer to a network.

NLRI

Network layer reachability information. In BGP, the system sends routing update messages containing NLRI to describe a route and how to get there. A **BGP** update message carries one or more NLRI prefixes and the attributes of a route for each NLRI prefix; the route attributes include a BGP next hop gateway address, community values, and other information.

NMS

Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.

node

In general networking terms, a node is a device on the network. In the Extreme Networks implementation, a node is a CPU that runs the management application on the switch. Each **MSM** on modular switches installed in the chassis is a node.

node manager

The node manager performs the process of node election, which selects the master, or primary, **MSM** when you have two MSMs installed in the modular chassis. The node manager is useful for system redundancy.

NSSA

Not-so-stubby area. In **OSPF**, NSSA is a stub area, which is connected to only one other area, with additional capabilities:

- External routes originating from an ASBR connected to the NSSA can be advertised within the NSSA.
- External routes originating from the NSSA can be propagated to other areas.

NTP

Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC 1305)

O**odometer**

In the Extreme Networks implementation, each field replaceable component contains a system odometer counter in EEPROM.

On modular switches, using the CLI, you can display how long each following individual component has been in service:

- chassis
- MSMs
- I/O modules
- power controllers

On standalone switches, you display the days of service for the switch.

OFDM

Orthogonal frequency division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels. OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.

OID

Object identifier.

option 82

This is a security feature that you configure as part of BOOTP/DHCP. Option 82 allows a server to bind the client's port, IP address, and MAC number for subscriber identification.

OSI

Open Systems Interconnection. OSI is an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.

OSI Layer 2

At the Data Link layer (OSI Layer 2), data packets are encoded and decoded into bits. The data link layer has two sub-layers:

- The Logical Link Control (LLC) layer controls frame synchronization, flow control and error checking.
- The Media Access Control (MAC) layer controls how a computer on the network gains access to the data and permission to transmit it.

OSI Layer 3

The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, inter-networking, error handling, congestion control and packet sequencing.

OSI reference model

The seven-layer standard model for network architecture is the basis for defining network protocol standards and the way that data passes through the network. Each layer specifies particular network functions; the highest layer is closest to the user, and the lowest layer is closest to the media carrying

the information. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user or program. This model is used worldwide for teaching and implementing networking protocols.

OSPF

Open Shortest Path First. An interior gateway routing protocol for TCP/IP networks, OSPF uses a link state routing algorithm that calculates routes for packets based on a number of factors, including least hops, speed of transmission lines, and congestion delays. You can also configure certain cost metrics for the algorithm. This protocol is more efficient and scalable than vector-distance routing protocols. OSPF features include least-cost routing, ECMP routing, and load balancing. Although OSPF requires CPU power and memory space, it results in smaller, less frequent router table updates throughout the network. This protocol is more efficient and scalable than vector-distance routing protocols.

OSPFv3

OSPFv3 is one of the routing protocols used with IPV6 and is similar to OSPF.

OUI

Organizational(ly) Unique Identifier. The OUI is the first 24 bits of a MAC address for a network device that indicate a specific vendor as assigned by IEEE.

P

packet

This is the unit of data sent across a network. Packet is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units. The packet is a group of bits, including data and control signals, arranged in a specific format. It usually includes a header, with source and destination data, and user data. The specific structure of the packet depends on the protocol used.

PAP

Password Authentication Protocol. This is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (See [CHAP](#).)

partner node

In [EAPS](#), the partner node is that end of the common link that is not a controller node; the partner node does not participate in any form of blocking.

PD

Powered device. In PoE, the PD is the powered device that plugs into the PoE switch.

PDU

Protocol data unit. A PDU is a message of a given protocol comprising payload and protocol-specific control information, typically contained in a header.

PEAP

Protected Extensible Authentication Protocol. PEAP is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user

authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP- Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also [EAP-TLS](#).)

PEC

Power Entry Circuit.

PEM

Power Entry Module.

PIM-DM

Protocol-Independent Multicast - Dense mode. PIM-DM is a multicast protocol that uses Reverse Path Forwarding but does not require any particular unicast protocol. It is used when recipients are in a concentrated area.

PIM-SM

Protocol-Independent Multicast - Sparse mode. PIM-SM is a multicast protocol that defines a rendezvous point common to both sender and receiver. Sender and receiver initiate communication at the rendezvous point, and the flow begins over an optimized path. It is used when recipients are in a sparse area.

ping

Packet Internet Groper. Ping is the [ICMP](#) echo message and its reply that tests network reachability of a device. Ping sends an echo packet to the specified host, waits for a response, and reports success or failure and statistics about its operation.

PKCS #8 (Public-Key Cryptography Standard #8)

One of several standard formats which can be used to store a private key in a file. It can optionally be encrypted with a password.

PKI

Public Key Infrastructure.

PMBR

PIM multicast border router. A PMBR integrates PIM-DM and PIM-SM traffic.

PoE

Power over Ethernet. The PoE standard (IEEE 802.3af) defines how power can be provided to network devices over existing Ethernet connections, eliminating the need for additional external power supplies.

policy files

You use policy files in ExtremeXOS to specify [ACLs](#) and policies. A policy file is a text file (with a .pol extension) that specifies a number of conditions to test and actions to take. For ACLs, this information is applied to incoming traffic at the hardware level. Policies are more general and can be applied to incoming routing information; they can be used to rewrite and modify routing advertisements.

port mirroring

Port mirroring configures the switch to copy all traffic associated with one or more ports to a designated monitor port. A packet bound for or heading away from the mirrored port is forwarded onto the monitor port as well. The monitor port can be connected to a network analyzer or RMON probe for packet analysis. Port mirroring is a method of monitoring network traffic that a network administrator uses as a diagnostic tool or debugging feature; it can be managed locally or remotely.

POST

Power On Self Test. On Extreme Networks switches, the POST runs upon powering-up the device. Once the hardware elements are determined to be present and powered on, the boot sequence begins. If the MGMT LED is yellow after the POST completes, contact your supplier for advice.

primary port

In **EAPS**, a primary port is a port on the master node that is designated the primary port to the ring.

protected VLAN

In **STP**, protected VLANs are the other (other than the carrier VLAN) VLANs that are members of the STPD but do not define the scope of the STPD. Protected VLANs do not transmit or receive STP BPDUs, but they are affected by STP state changes and inherit the state of the carrier VLAN. Also known as non-carrier VLANs, they carry the data traffic.

In **EAPS**, a protected VLAN is a VLAN that carries data traffic through an EAPS domain. You must configure one or more protected VLANs for each EAPS domain. This is also known as a data VLAN.

proxy ARP

This is the technique in which one machine, usually a router, answers ARP requests intended for another machine. By masquerading its identity (as an endstation), the router accepts responsibility for routing packets to the real destination. Proxy ARP allows a site to use a single IP address with two physical networks. Subnetting is normally a better solution.

pseudowire

Sometimes spelled as "pseudo-wire" or abbreviated as PW. As described in RFC 3985, there are multiple methods for carrying networking services over a packet-switched network. In short, a pseudowire emulates networking or telecommunication services across packet-switched networks that use Ethernet, IP, or MPLS. Emulated services include T1 leased line, frame relay, Ethernet, ATM, TDM, or SONET/SDH.

push-to-talk (PTT)

The push-to-talk is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic.

A PTT call is initiated by selecting a channel and pressing the 'talk' key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.

PVST+

Per VLAN Spanning Tree +. This implementation of STP has a 1:1 relationship with VLANs. The Extreme Networks implementation of PVST+ allows you to interoperate with third-party devices running this version of STP. PVST is an earlier version of this protocol and is compatible with PVST+.

Q

QoS

Quality of Service. Policy-enabled QoS is a network service that provides the ability to prioritize different types of traffic and to manage bandwidth over a network. QoS uses various methods to prioritize traffic, including IEEE 802.1p values and IP DiffServ values. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, and setting traffic priorities across the network. (RFC 2386)

R

radar

Radar is a set of advanced, intelligent, Wireless-Intrusion-Detection-Service-Wireless-Intrusion-Prevention-Service (WIDS-WIPS) features that are integrated into the Wireless Controller and its access points (APs). Radar provides a basic solution for discovering unauthorized devices within the wireless coverage area. Radar performs basic RF network analysis to identify unmanaged APs and personal ad-hoc networks. The Radar feature set includes: intrusion detection, prevention and interference detection.

RADIUS

Remote Authentication Dial In User Service. RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

RARP

Reverse ARP. Using this protocol, a physical device requests to learn its IP address from a gateway server's ARP table. When a new device is set up, its RARP client program requests its IP address from the RARP server on the router. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

rate limiting

In [QoS](#), rate limiting is the process of restricting traffic to a peak rate (PR). For more information, see rate limiting and rate shaping in the [ExtremeXOS 21.1 User Guide](#).

rate shaping

In [QoS](#), rate shaping is the process of reshaping traffic throughput to give preference to higher priority traffic or to buffer traffic until forwarding resources become available. For more information, see rate limiting and rate shaping in the [ExtremeXOS 21.1 User Guide](#).

RF

Radio Frequency. A frequency in the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that can propagate through space. These frequencies in the electromagnetic spectrum range from Ultra-low frequency (ULF): 0-3 Hz to Extremely high frequency (EHF): 30 GHz-300 GHz. The middle ranges are: Low frequency (LF): 30 kHz-300 kHz; Medium frequency (MF): 300 kHz-3 MHz; High frequency (HF): 3

MHz–30 MHz; Very high frequency (VHF): 30 MHz–300 MHz; and Ultra-high frequency (UHF): 300 MHz–3 GHz.

RFC

Request for Comment. The IETF RFCs describe the definitions and parameters for networking. The RFCs are catalogued and maintained on the IETF RFC website: www.ietf.org/rfc.html.

Ridgeline

Ridgeline is an Extreme Networks-proprietary graphical user interface (GUI) network management system. The name was changed from EPICenter to Ridgeline in 2011.

RIP

Routing Information Protocol. This IGP vector-distance routing protocol is part of the TCP/IP suite and maintains tables of all known destinations and the number of hops required to reach each. Using RIP, routers periodically exchange entire routing tables. RIP is suitable for use only as an IGP.

RIPng

RIP next generation. RIPng is one of the routing protocols used with IPv6 and is similar to RIP.

RMON

Remote monitoring. RMON is a standardized method to make switch and router information available to remote monitoring applications. It is an SNMP network management protocol that allows network information to be gathered remotely. RMON collects statistics and enables a management station to monitor network devices from a central location. It provides multivendor interoperability between monitoring devices and management stations. RMON is described in several RFCs (among them IETF RFC 1757 and RFC 2201).

Network administrators use RMON to monitor, analyze, and troubleshoot the network. A software agent can gather the information for presentation to the network administrator with a graphical user interface (GUI). The administrator can find out how much bandwidth each user is using and what web sites are being accessed; you can also set alarms to be informed of potential network problems.

roaming

In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) -identified by its SSID.

root bridge

In **STP**, the root bridge is the bridge with the best bridge identifier selected to be the root bridge. The network has only one root bridge. The root bridge is the only bridge in the network that does not have a root port.

root port

In **STP**, the root port provides the shortest path to the root bridge. All bridges except the root bridge contain one root port.

route aggregation

In **BGP**, you can combine the characteristics of several routes so they are advertised as a single route, which reduces the size of the routing tables.

route flapping

A route is flapping when it is repeatedly available, then unavailable, then available, then unavailable. In the ExtremeXOS BGP implementation, you can minimize the route flapping using the route flap dampening feature.

route reflector

In BGP, you can configure the routers within an AS such that a single router serves as a central routing point for the entire AS.

routing confederation

In BGP, you can configure a fully meshed autonomous system into several sub-ASs and group these sub-ASs into a routing confederation. Routing confederations help with the scalability of BGP.

RP-SMA

Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas.

RSN

Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

RSSI

RSSI received signal strength indication (in 802.11 standard).

RTS/CTS

RTS request to send, CTS clear to send (in 802.11 standard).

RSTP

Rapid Spanning Tree Protocol. RSTP, described in IEEE 802.1w, is an enhanced version of STP that provides faster convergence. The Extreme Networks implementation of RSTP allows seamless interoperability with legacy STP.

S**SA**

Source address. The SA is the IP or MAC address of the device issuing the packet.

SCP

Secure Copy Protocol. SCP2, part of SSH2, is used to transfer configuration and policy files.

SDN

Software-defined Networking. An approach to computer networking that seeks to manage network services through decoupling the system that makes decisions about where traffic is sent (control plane) from the underlying systems that forward traffic to the selected destination (data plan).

secondary port

In EAPS, the secondary port is a port on the master node that is designated the secondary port to the ring. The transit node ignores the secondary port distinction as long as the node is configured as a transit node.

segment

In Ethernet networks, a section of a network that is bounded by bridges, routers, or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.

server certificate

A certificate identifying a server. When a client connects to the server, the server sends its certificate to the client and the client validates the certificate to trust the server.

sFlow

sFlow allows you to monitor network traffic by statistically sampling the network packets and periodically gathering the statistics. The sFlow monitoring system consists of an sFlow agent (embedded in a switch, router, or stand-alone probe) and an external central data collector, or sFlow analyzer.

SFP

Small form-factor pluggable. These transceivers offer high speed and physical compactness.

slow path

This term refers to the data path for packets that must be processed by the switch CPU, whether these packets are generated by the CPU, removed from the network by the CPU, or simply forwarded by the CPU.

SLP

Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network.

Using SLP, networking applications can discover the existence, location and configuration of networked devices.

With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.

For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.

(SLP version 2, RFC2608, updating RFC2165)

SMF

Single-mode fiber. SMF is a laser-driven optical fiber with a core diameter small enough to limit transmission to a single bound mode. SMF is commonly used in long distance transmission of more than three miles; it sends one transmission at a time.

SMI

Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC 1155 and RFC 1442 (SNMPv2).

SMON

Switch Network Monitoring Management (MIB) system defined by the IETF document RFC 2613. SMON is a set of MIB extensions for RMON that allows monitoring of switching equipment from a SNMP Manager in greater detail.

SMT

Station Management. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are:

- dot11smt—objects related to station management and local configuration
- dot11mac—objects that report/configure on the status of various MAC parameters
- dot11res—objects that describe available resources
- dot11phy—objects that report on various physical items

SNMP

Simple Network Management Protocol. SNMP is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SNTP

Simple Network Time Protocol. SNTP is used to synchronize the system clocks throughout the network. An extension of the Network Time Protocol, SNTP can usually operate with a single server and allows for IPv6 addressing.

SSH

Secure Shell, sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol of securely gaining access to a remote computer. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. At Extreme Networks, the SSH is a separate software module, which must be downloaded separately. (SSH is bundled with SSL in the software module.)

SSID

Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSSs). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS.

In 802.11 networks, each access point (AP) advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named access point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID. Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

SSL

Secure Sockets Layer. SSL is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the

public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

spoofing

Hijacking a server's IP address or hostname so that requests to the server are redirected to another server. Certificate validation is used to detect and prevent this.

standard mode

Use ESRP standard mode if your network contains switches running ExtremeWare and switches running ExtremeXOS, both participating in ESRP.

STP

Spanning Tree Protocol. STP is a protocol, defined in IEEE 802.1d, used to eliminate redundant data paths and to increase network efficiency. STP allows a network to have a topology that contains physical loops; it operates in bridges and switches. STP opens certain paths to create a tree topology, thereby preventing packets from looping endlessly on the network. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the STP topology and re-establishes the link by activating the standby path.

STPD

Spanning Tree Domain. An STPD is an STP instance that contains one or more VLANs. The switch can run multiple STPDs, and each STPD has its own root bridge and active path. In the Extreme Networks implementation of STPD, each domain has a carrier VLAN (for carrying STP information) and one or more protected VLANs (for carrying the data).

STPD mode

The mode of operation for the STPD. The two modes of operation are:

- 802.1d—Compatible with legacy STP and other devices using the IEEE 802.1d standard.
- 802.1w—Compatible with Rapid Spanning Tree (RSTP).

stub areas

In [OSPF](#), a stub area is connected to only one other area (which can be the backbone area). External route information is not distributed to stub areas.

subnet mask

See [netmask](#).

subnets

Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.

superloop

In [EAPS](#), a superloop occurs if the common link between two EAPS domains goes down and the master nodes of both domains enter the failed state putting their respective secondary ports into the

forwarding state. If there is a data VLAN spanning both EAPS domains, this action forms a loop between the EAPS domains.

SVP

SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

syslog

A protocol used for the transmission of **event** notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

system health check

The primary responsibility of the system health checker is to monitor and poll error registers. In addition, the system health checker can be enabled to periodically send diagnostic packets. System health check errors are reported to the syslog.

T

TACACS+

Terminal Access Controller Access Control System. Often run on UNIX systems, the TACAS+ protocol provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services. User passwords are administered in a central database rather than in individual routers, providing easily scalable network security solutions.

tagged VLAN

You identify packets as belonging to the same tagged VLAN by putting a value into the 12-bit (4 octet) VLAN ID field that is part of the IEEE 802.1Q field of the header. Using this 12-bit field, you can configure up to 4096 individual VLAN addresses (usually some are reserved for system VLANs such as management and default VLANs); these tagged VLANs can exist across multiple devices. The tagged VLAN can be associated with both tagged and untagged ports.

TCN

Topology change notification. The TCN is a timer used in **RSTP** that signals a change in the topology of the network.

TCP / IP

Transmission Control Protocol. Together with Internet Protocol (IP), TCP is one of the core protocols underlying the Internet. The two protocols are usually referred to as a group, by the term TCP/IP. TCP provides a reliable connection, which means that each end of the session is guaranteed to receive all of the data transmitted by the other end of the connection, in the same order that it was originally transmitted without receiving duplicates.

TFTP

Trivial File Transfer Protocol. TFTP is an Internet utility used to transfer files, which does not provide security or directory listing. It relies on [UDP](#).

TKIP

Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. The protocol's enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (re-keyed) automatically and authenticated between devices after the re-key interval (either a specified period of time, or after a specified number of packets has been transmitted).

TLS

Transport Layer Security. See [SSL](#).

ToS / DSCP

ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP box contained in the IP header of a frame is used by applications to indicate the priority and [Quality of Service](#) for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.

transit node

In [EAPS](#), the transit node is a switch, or node, that is not designated a master in the EAPS domain ring.

truststore

A repository containing trusted certificates, used to validate an incoming certificate. A truststore usually contains CA certificates, which represent certificate authorities that are trusted to sign certificates, and can also contain copies of server or client certificates that are to be trusted when seen.

TSN

Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

Time-Sensitive Networking. Standards under development by the Time-Sensitive Networking task group of the IEEE 802.1 working group. There are various characteristics of TSN, including packet preemption, prioritized packet queuing, congestion control, bandwidth reservation, and transmit latency determination used to guarantee that data packets always arrive within a certain predetermined window of time.

tunnelling

Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.

U

U-NII

Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.

UDP

User Datagram Protocol. This is an efficient but unreliable, connectionless protocol that is layered over IP (as is [TCP](#)). Application programs must supplement the protocol to provide error processing and retransmitting data. UDP is an OSI Layer 4 protocol.

unicast

A unicast packet is communication between a single sender and a single receiver over a network.

untagged VLAN

A VLAN remains untagged unless you specifically configure the IEEE 802.1Q value on the packet. A port cannot belong to more than one untagged VLAN using the same protocol.

USM

User-based security model. In SNMPv3, USM uses the traditional SNMP concept of user names to associate with security levels to support secure network management.

V

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.

VEPA

Virtual Ethernet Port Aggregator. This is a Virtual Machine (VM) server feature that works with the ExtremeXOS Direct Attach Feature to support communications between VMs.

virtual link

In [OSPF](#), when a new area is introduced that does not have a direct physical attachment to the backbone, a virtual link is used. Virtual links are also used to repair a discontinuous backbone area.

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.

virtual router MAC address

In VRRP, RFC 2338 assigns a static MAC address for the first five octets of the VRRP virtual router. These octets are set to 00-00-5E-00-01. When you configure the VRRP VRID, the last octet of the MAC address is dynamically assigned the VRID number.

VLAN

Virtual LAN. The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.

VLSM

Variable-length subnet masks. In [OSPF](#), VLSMs provide subnets of different sizes within a single IP block.

VM

Virtual Machine. A VM is a logical machine that runs on a VM server, which can host multiple VMs.

VMAN

Virtual MAN. In ExtremeXOS software, VMANs are a bi-directional virtual data connection that creates a private path through the public network. One VMAN is completely isolated from other VMANs; the encapsulation allows the VMAN traffic to be switched over Layer 2 infrastructure. You implement VMAN using an additional 892.1Q tag and a configurable EtherType; this feature is also known as Q-in-Q switching.

VNS

Virtual Network Services. An Extreme Networks-specific technique that provides a means of mapping wireless networks to a wired topology.

VoIP

Voice over Internet Protocol is an Internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet, and is reassembled when it reaches the destination.

VPN

Virtual private network. A VPN is a private network that uses the public network (Internet) to connect remote sites and users. The VPN uses virtual connections routed through the Internet from a private network to remote sites or users. There are different kinds of VPNs, which all serve this purpose. VPNs also enhance security.

VR-Control

This virtual router (VR) is part of the embedded system in Extreme Networks switches. VR-Control is used for internal communications between all the modules and subsystems in the switch. It has no ports, and you cannot assign any ports to it. It also cannot be associated with VLANs or routing protocols. (Referred to as VR-1 in earlier ExtremeXOS software versions.)

VR-Default

This VR is part of the embedded system in Extreme Networks switches. VR-Default is the default VR on the system. All data ports in the switch are assigned to this VR by default; you can add and delete ports from this VR. Likewise, VR-Default contains the default VLAN. Although you cannot delete the default VLAN from VR-Default, you can add and delete any user-created VLANs. One instance of each routing protocol is spawned for this VR, and they cannot be deleted. (Referred to as VR-2 in earlier ExtremeXOS software versions.)

VR-Mgmt

This VR is part of the embedded system in Extreme Networks switches. VR-Mgmt enables remote management stations to access the switch through Telnet, SSH, or SNMP sessions; and it owns the management port. The management port cannot be deleted from this VR, and no other ports can be added. The Mgmt VLAN is created VR-Mgmt, and it cannot be deleted; you cannot add or delete any other VLANs or any routing protocols to this VR. (Referred to as VR-0 in earlier ExtremeXOS software versions.)

VRID

In VRRP, the VRID identifies the VRRP virtual router. Each VRRP virtual router is given a unique VRID. All the VRRP routers that participate in the VRRP virtual router are assigned the same VRID.

VRRP

Virtual Router Redundancy Protocol. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the master router, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the master router become unavailable. In case the master router fails, the virtual IP address is mapped to a backup router's IP address; this backup becomes the master router. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every host. VRRP is defined in RFC 2338.

VRRP router

Any router that is running VRRP. A VRRP router can participate in one or more virtual routers with VRRP; a VRRP router can be a backup router for one or more master routers.

VSA

Vendor Specific Attribute. An attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC 2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

W

walled garden

A restricted subset of network content that wireless devices can access.

WEP

Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

WINS

Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.

WLAN

Wireless Local Area Network.

WMM

Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This standard is compliant with the IEEE 802.11e [Quality of Service](#) extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.

WPA

Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEP's basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. [Certificate Authentication](#) (CA) can also be used. Also part of the encryption mechanism are 802.1x for dynamic key distribution and Message Integrity Check (MIC) a.k.a. Michael.

WPA requires that all computers and devices have WPA software.

WPA-PSK

Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the AP or router and the WPA clients.

This pre-shared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic re-keying.

X

XENPAK

Pluggable optics that contain a 10 Gigabit Ethernet module. The XENPAKs conform to the IEEE 802.3ae standard.

XNV

Extreme Network Virtualization. This ExtremeXOS feature enables the software to support VM port movement, port configuration, and inventory on network switches.