



IdentiFi Wireless User Guide

Release V9.21.01

Copyright © 2012–2016 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, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

Table of Contents

Legal Notices.....	0
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
Extreme Networks® License Agreement.....	14
Chapter 2: Overview of the Extreme Networks IdentiFi Wireless Solution.....	21
Introduction.....	21
Conventional Wireless LANs.....	22
Elements of the Extreme Networks IdentiFi Wireless Solution.....	22
Extreme Networks IdentiFi Wireless and Your Network.....	26
IdentiFi Wireless Appliance Product Family.....	36
Chapter 3: Configuring the IdentiFi Wireless Appliance.....	38
System Configuration Overview.....	38
Logging on to the IdentiFi Wireless Appliance.....	40
Wireless Assistant Home Screen.....	41
Working with the Basic Installation Wizard.....	45
Configuring the IdentiFi Wireless Appliance for the First Time.....	51
Using an AeroScout/Ekahau Location-based Solution.....	96
Additional Ongoing Operations of the System.....	99
Chapter 4: Configuring the IdentiFi Wireless APs.....	100
Wireless AP Overview.....	100
Discovery and Registration Overview.....	112
Wireless AP Default Configuration.....	119
Configuring Wireless AP Properties.....	136
Configuring Wireless AP Radio Properties.....	147
Configuring VLAN Tags for Wireless APs.....	161
Setting Up 802.1x Authentication for a Wireless AP.....	162
Configuring Co-Located APs in Load Balance Groups.....	170
Configuring an AP Cluster.....	177
Configuring an AP as a Sensor.....	178
Configuring an AP as a Guardian.....	180
Performing AP Software Maintenance.....	181
Understanding the IdentiFi Wireless AP LED Status.....	185
Chapter 5: Configuring Topologies.....	209
Topology Overview.....	209
Configuring the Admin Port.....	210
Configuring a Basic Data Port Topology.....	212
Creating a Topology Group.....	215

Enabling Management Traffic.....	216
Layer 3 Configuration.....	217
Exception Filtering.....	223
Multicast Filtering.....	226
Chapter 6: Configuring Roles.....	228
Roles Overview.....	228
Configuring Default VLAN and Class of Service for a Role.....	228
Policy Rules.....	230
Chapter 7: Configuring WLAN Services.....	243
WLAN Services Overview.....	243
Third-party AP WLAN Service Type.....	244
Configuring a Basic WLAN Service.....	244
Configuring Privacy.....	250
Configuring Accounting and Authentication.....	257
Configuring QoS Modes.....	284
Chapter 8: Configuring a VNS.....	290
Configuring a VNS.....	290
VNS Global Settings.....	292
Methods for Configuring a VNS.....	314
Manually Creating a VNS.....	315
Creating a VNS Using the Wizard.....	316
Enabling and Disabling a VNS.....	377
Renaming a VNS.....	378
Deleting a VNS.....	378
Chapter 9: Configuring Classes of Service.....	379
Classes of Service Overview.....	379
Configuring Classes of Service.....	379
CoS Rule Classification.....	382
Priority and ToS/DSCP Marking.....	383
Rate Limiting.....	384
Chapter 10: Configuring Sites.....	386
VNS Sites Overview.....	386
Configuring Sites.....	386
Recommended Deployment Guidelines.....	387
Radius Configuration.....	391
Selecting AP Assignments.....	392
Selecting WLAN Assignments.....	393
Chapter 11: Working with a Mesh Network.....	395
About Mesh.....	395
Simple Mesh Configuration.....	395
Wireless Repeater Configuration.....	396
Wireless Bridge Configuration.....	397
Examples of Deployment.....	398
Mesh WLAN Services.....	398
Key Features of Mesh.....	402
Deploying the Mesh System.....	404
Changing the Pre-shared Key in a Mesh WLAN Service.....	410

Chapter 12: Working with a Wireless Distribution System.....	411
About WDS.....	411
Simple WDS Configuration.....	411
Wireless Repeater Configuration.....	412
Wireless Bridge Configuration.....	413
Examples of Deployment.....	414
WDS WLAN Services.....	414
Key Features of WDS.....	418
Deploying the WDS System.....	421
Changing the Pre-shared Key in a WDS WLAN Service.....	429
Chapter 13: Availability and Session Availability.....	430
Availability.....	430
Session Availability.....	438
Viewing SLP Activity.....	446
Chapter 14: Configuring Mobility.....	448
Mobility Overview.....	448
Mobility Domain Topologies.....	449
Configuring a Mobility Domain.....	451
Chapter 15: Working with Third-party APs.....	454
Defining Authentication by Captive Portal for the Third-party AP WLAN Service.....	454
Defining the Third-party APs List.....	454
Defining Policy Rules for the Third-party APs.....	454
Chapter 16: Working with Identifi Radar.....	456
Radar Overview.....	456
Radar Components.....	457
Radar License Requirements.....	458
Radar Scan Profiles.....	459
Viewing Existing Scan Profiles.....	460
Enabling the Analysis and Data Collector Engines.....	462
Adding a New Scan Profile.....	463
Configuring a Legacy Scan Profile.....	464
Configuring an In-Service Scan Profile.....	467
Configuring a Guardian Scan Profile.....	472
Maintaining the Radar Lists of APs.....	477
Configuring the Location Engine.....	486
Working with Radar Reports.....	493
Chapter 17: Working with Reports and Statistics.....	504
Available Reports and Statistics.....	504
Viewing AP Reports and Statistics.....	504
Viewing Active Clients.....	518
Viewing Role Filter Statistics.....	520
Viewing Topology Reports.....	522
Viewing Mobility Reports.....	525
Viewing Controller Status Information.....	528
Viewing Routing Protocol Reports.....	532
Viewing RADIUS Reports.....	535
Call Detail Records (CDRs).....	538

Chapter 18: Performing System Administration.....	544
Performing Wireless AP Client Management.....	544
Defining Wireless Assistant Administrators and Login Groups.....	549
Chapter 19: Logs, Traces, Audits and DHCP Messages.....	552
IdentiFi Wireless Appliance Messages.....	552
Working with Logs.....	552
Viewing Wireless AP Traces.....	560
Viewing Audit Messages.....	561
Viewing the DHCP Messages.....	562
Viewing the NTP Messages.....	563
Viewing Software Upgrade Messages.....	564
Viewing Configuration Restore/Import Messages.....	565
Chapter 20: Working with GuestPortal Administration.....	567
About GuestPortals.....	567
Adding New Guest Accounts.....	567
Enabling or Disabling Guest Accounts.....	570
Editing Guest Accounts.....	570
Removing Guest Accounts.....	571
Importing and Exporting a Guest File.....	572
Viewing and Printing a GuestPortal Account Ticket.....	575
Working with the GuestPortal Ticket Page.....	577
Configuring Web Session Timeouts.....	578
Appendix A: Glossary.....	580
A.....	580
B.....	583
C.....	584
D.....	589
E.....	592
F.....	596
G.....	598
H.....	599
I.....	600
J.....	604
L.....	604
M.....	606
N.....	610
O.....	611
P.....	613
Q.....	616
R.....	617
S.....	620
T.....	624
U.....	626
V.....	627
W.....	630
X.....	631
Appendix B: Regulatory Information.....	632

IdentiFi Wireless APs 37XX and 38XX..... 632
IdentiFi Wireless APs 26XX and 36XX..... 633
Appendix C: Default GuestPortal Ticket Page..... 648
Ticket Page..... 648



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](#)
[Extreme Networks License Agreement](#)

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

To Access the Online Help System:

- 1 In the Identifi Wireless Assistant top menu bar, click **Help**.
- 2 The online help system is launched.

Intended Audience

This guide is a reference for system administrators who install and manage the Identifi Wireless 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 Extreme Networks Identifi Wireless Solution on page 21
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 Identifi Wireless Appliance on page 38

For...	Refer to...
Information on how to install the IdentifiFi Wireless AP, how it discovers and registers with the controller, and how to view and modify radio configuration.	Configuring the IdentifiFi Wireless APs on page 100
An overview of topologies and provides detailed information about how to configure them.	Configuring Topologies on page 209
An overview of roles and provides detailed information about how to configure them.	Configuring Roles on page 228
An overview of WLAN services and provides detailed information about how to configure them.	Configuring WLAN Services on page 243
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 290
Information about configuring Classes of Service (CoS) 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 379
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 386
An overview of Mesh networks and provides detailed information about how to create a Mesh network.	Working with a Mesh Network on page 395
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 411
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 430
Information on how to set up the mobility domain that provides mobility for a wireless device user when the user roams from one IdentifiFi Wireless AP to another in the mobility domain.	Configuring Mobility on page 448
Information on how to use the IdentifiFi Wireless features with third-party wireless access points.	Working with Third-party APs on page 454
Information on the security tool that scans for, detects, provides countermeasures, and reports on rogue APs.	Working with IdentifiFi Radar on page 456
Information on the various reports and displays available in the system.	Working with Reports and Statistics on page 504
Information on system administration activities, such as performing IdentifiFi Wireless AP client management, defining management users, configuring the network time, and configuring Web session timeouts.	Performing System Administration on page 544
Information on how to view and interpret the logs, traces, audits and DHCP messages.	Logs, Traces, Audits and DHCP Messages on page 552
Information on how to configure GuestPortal accounts.	Working with GuestPortal Administration on page 567

For...	Refer to...
A list of terms and definitions for the IdentiFi Wireless Appliance and the IdentiFi Wireless AP as well as standard industry terms used in this guide.	Glossary
Regulatory information for the IdentiFi Wireless Appliances and the IdentiFi Wireless APs.	Regulatory Information on page 632
The default GuestPortal ticket page source code.	Default GuestPortal Ticket Page on page 648

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 IdentiFi Wireless 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, tricks, 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 Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size 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 previous Return Material Authorization (RMA) numbers

Related Publications

IdentiFi Wireless Appliance and Access Point documentation can be found on the Extreme Extranet site (<http://extranet.extremenetworks.com>), which requires a login account.

Extreme recommends the following guides for users of wireless products:

- [IdentiFi Wireless CLI Reference Guide](#)
- [IdentiFi Wireless Getting Started Guide](#)
- [IdentiFi Wireless Integration Guide](#)
- [IdentiFi Wireless Maintenance Guide](#)
- [IdentiFi Wireless Open Source Declaration](#)
- [IdentiFi Wireless User Guide](#)

Extreme Networks® License Agreement

This document is an agreement (“Agreement”) between You, the end user, and Extreme Networks, Inc., on behalf of itself and its Affiliates (“Extreme”) that sets forth your rights and obligations with respect

to the “Licensed Materials”. BY INSTALLING SOFTWARE AND/OR THE LICENSE KEY FOR THE SOFTWARE (“License Key”) (collectively, “Licensed Software”), IF APPLICABLE, COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE AND/OR ANY OF THE LICENSED MATERIALS UNDER THIS AGREEMENT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE(S) AND THE LIMITATION(S) OF WARRANTY AND DISCLAIMER(S)/ LIMITATION(S) OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY (IF APPLICABLE) TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND/OR LICENSED MATERIALS AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT TO ARRANGE FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn:

legalteam@extremenetworks.com.

- 1 DEFINITIONS. “Affiliates” means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. “Server Application” means the software application associated to software authorized for installation (per License Key, if applicable) on one or more of Your servers as further defined in the Ordering Documentation. “Client Application” shall refer to the application to access the Server Application. “Network Device”, for purposes of this Agreement, shall mean a physical computer device, appliance, appliance component, controller, wireless access point, or virtual appliance as further described within the applicable product documentation, which includes the Order Documentation. “Licensed Materials” means the Licensed Software (including the Server Application and Client Application), Network Device (if applicable), Firmware, media embodying software, and the accompanying documentation. “Concurrent User” shall refer to any of Your individual employees who You provide access to the Server Application at any one time. “Firmware” refers to any software program or code embedded in chips or other media. “Standalone” software is software licensed for use independent of any hardware purchase as identified in the Ordering Documentation. “Licensed Software” collectively refers to the software, including Standalone software, Firmware, Server Application, Client Application or other application licensed with conditional use parameters as defined in the Ordering Documentation. “Ordering Documentation” shall mean the applicable price quotation, corresponding purchase order, relevant invoice, order acknowledgement, and accompanying documentation or specifications for the products and services purchased, acquired or licensed hereunder from Extreme either directly or indirectly.
- 2 TERM. This Agreement is effective from the date on which You accept the terms and conditions of this Agreement via click-through, commence using the products and services or upon delivery of the License Key if applicable, and shall be effective until terminated. In the case of Licensed Materials offered on a subscription basis, the term of “licensed use” shall be as defined within Your Ordering Documentation.
- 3 GRANT OF LICENSE. Extreme will grant You a non-transferable, non-sublicensable, non-exclusive license to use the Licensed Materials and the accompanying documentation for Your own business purposes subject to the terms and conditions of this Agreement, applicable licensing restrictions, and any term, user server networking device, field of use, or other restrictions as set forth in Your Ordering Documentation. If the Licensed Materials are being licensed on a subscription and/or capacity basis, the applicable term and/or capacity limit of the license shall be specified in Your Ordering Documentation. You may install and use the Licensed Materials as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4 LICENSE TYPES.

- *Single User, Single Network Device.* Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials as bundled with a single Network Device as identified by a unique serial number for the applicable Term, if and as specified in Your Ordering Documentation, or any replacement for that network device for that same Term, for internal use only. A separate license, under a separate License Agreement, is required for any other network device on which You or another individual, employee or other third party intend to use the Licensed Materials. A separate license under a separate License Agreement is also required if You wish to use a Client license (as described below).
- *Single User, Multiple Network Device.* Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials with a defined amount of Network Devices as defined in the Ordering Documentation.
- *Client.* Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Materials on your server and allow the specific number of Concurrent Users as ordered by you and is set forth in Your Ordering Documentation. A separate license is required for each additional Concurrent User.
- *Standalone.* Software or other Licensed Materials licensed to You for use independent of any Network Device.
- *Subscription.* Licensed Materials, and inclusive Software, Network Device or related appliance updates and maintenance services, licensed to You for use during a subscription period as defined in Your applicable Ordering Documentation.
- *Capacity.* Under the terms of this license, the license granted to You by Extreme authorizes You to use the Licensed Materials up to the amount of capacity or usage as defined in the Ordering Documentation.

5 AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, Extreme reserves the right to charge You for all reasonable expenses related to such audit in addition to any other liabilities and overages applicable as a result of such non-compliance, including but not limited to additional fees for Concurrent Users, excess capacity or usage over and above those specifically granted to You. From time to time, the Licensed Materials may upload information about the Licensed Materials and the associated usage to Extreme. This is to verify the Licensed Materials are being used in accordance with a valid license and/or entitlement. By using the Licensed Materials, you consent to the transmission of this information.

6 RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Materials, including the Licensed Software, or to translate the Licensed Materials into another computer language. The media embodying the Licensed Materials may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme' prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. Any portion of the Licensed

Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7 TITLE AND PROPRIETARY RIGHTS

- a The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.
- b You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

- 8 PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme' exclusive property, and You shall use all commercially reasonable efforts to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme' prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Materials on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

- 9 MAINTENANCE AND UPDATES. Except as otherwise defined below, updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide updates, modifications, or enhancements, or maintenance and support services for the Licensed Materials to You. If you have purchased Licensed Materials on a subscription basis then the applicable service terms for Your Licensed Materials are as provided in Your Ordering Documentation. Extreme will perform the maintenance and updates in a timely and professional manner, during the Term of Your subscription, using qualified and experienced personnel. You will

cooperate in good faith with Extreme in the performance of the support services including, but not limited to, providing Extreme with: (a) access to the Extreme Licensed Materials (and related systems); and (b) reasonably requested assistance and information. Further information about the applicable maintenance and updates terms can be found on Extreme's website at <http://www.extremenetworks.com/company/legal/terms-of-support10>. **DEFAULT AND TERMINATION.** In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.

a Immediately after any termination of the Agreement, Your licensed subscription term, or if You have for any reason discontinued use of Licensed Materials, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Materials, including any Licensed Software, from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.

b Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

10 **DEFAULT AND TERMINATION.** In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.

a Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.

b Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11 **EXPORT REQUIREMENTS.** You are advised that the Licensed Materials, including the Licensed Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Licensed Materials, including the Licensed Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

12 **UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13 **LIMITED WARRANTY AND LIMITATION OF LIABILITY.** Extreme warrants to You that (a) the initially-shipped version of the Licensed Materials will materially conform to the Documentation; and (b) the media on which the Licensed Software is recorded will be free from material defects for a period of

ninety (90) days from the date of delivery to You or such other minimum period required under applicable law. Extreme does not warrant that Your use of the Licensed Materials will be error-free or uninterrupted.

NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

- 14 JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
- 15 FREE AND OPEN SOURCE SOFTWARE. Portions of the Software (Open Source Software) provided to you may be subject to a license that permits you to modify these portions and redistribute the modifications (an Open Source License). Your use, modification and redistribution of the Open Source Software are governed by the terms and conditions of the applicable Open Source License. More details regarding the Open Source Software and the applicable Open Source Licenses are available at www.extremenetworks.com/services/SoftwareLicensing.aspx. Some of the Open Source software may be subject to the GNU General Public License v.x (GPL) or the Lesser General Public Library (LGPL), copies of which are provided with the

Licensed Materials and are further available for review at www.extremenetworks.com/services/SoftwareLicensing.aspx, or upon request as directed herein. In accordance with the terms of the GPL and LGPL, you may request a copy of the relevant source code. See the Software Licensing web site for additional details. This offer is valid for up to three years from the date of original download of the software.

- 16 GENERAL.
- a This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
 - b This Agreement may not be changed or amended except in writing signed by both parties hereto.
 - c You represent that You have full right and/or authorization to enter into this Agreement.

- d This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme' assignees, licensors, and licensees.
- e Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.
- f The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.
- g Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.
- h (h) Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 United States
ATTN: Legal Department

2 Overview of the Extreme Networks IdentiFi Wireless Solution

Introduction

Conventional Wireless LANs

Elements of the Extreme Networks IdentiFi Wireless Solution

Extreme Networks IdentiFi Wireless and Your Network

IdentiFi Wireless Appliance Product Family

Introduction

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

The IdentiFi Wirelesscontroller 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 IdentiFi WirelessSystem.

The IdentiFi Wireless Appliance

The IdentiFi Wireless 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.

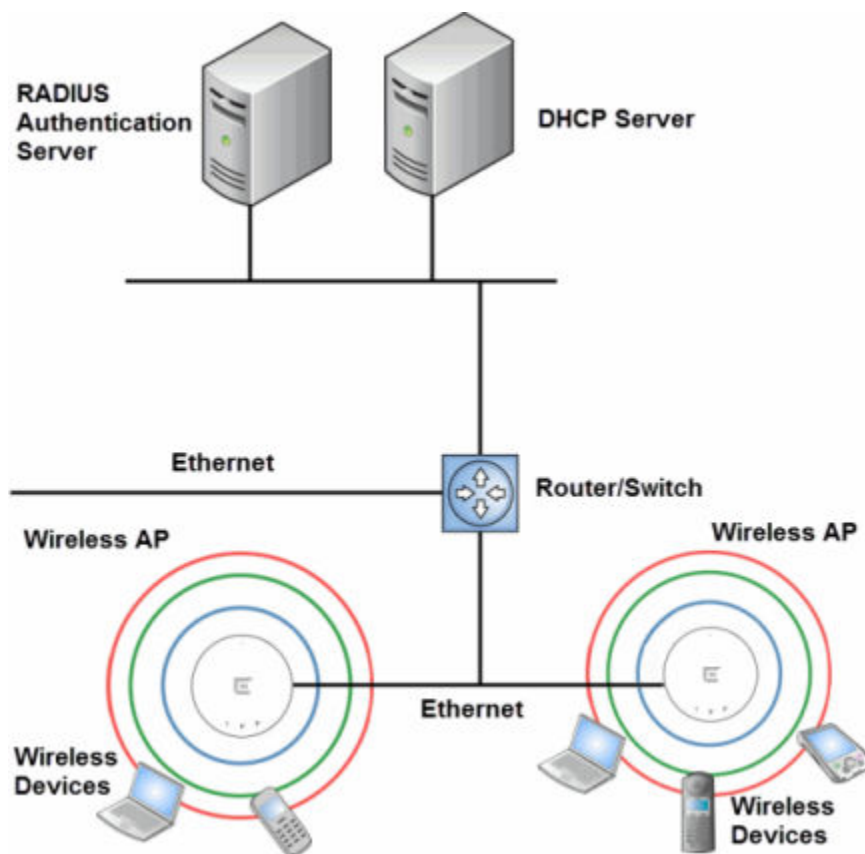


Figure 1: Standard Wireless Network Solution Example

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 Extreme Networks IdentiFi Wireless Solution

The Extreme Networks IdentiFi Wireless solution consists of two devices:

- IdentifiFi Wireless Appliance
- IdentifiFi Wireless AP

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

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

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

- RADIUS Server (Remote Access Dial-In User Service) or other authentication server
- DHCP 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 56.
- SLP (Service Location Protocol)

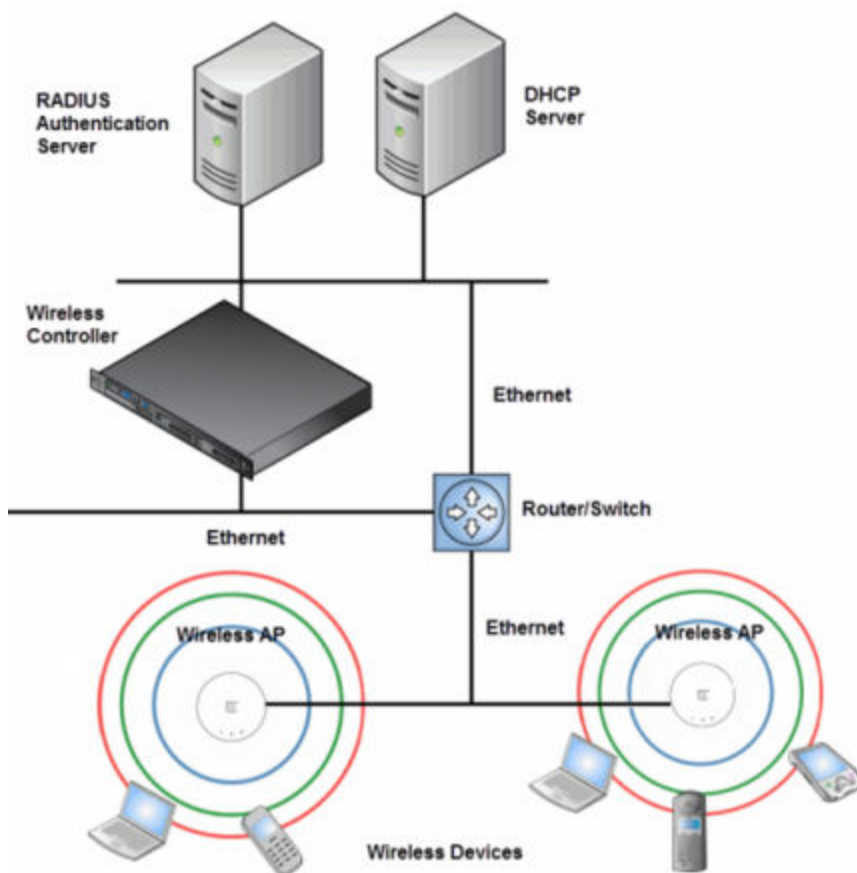


Figure 2: IdentifiFi Wireless Appliance Solution

As illustrated [above](#), the IdentifiFi Wireless 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 IdentifiFi Wireless system:

- Scales up to Enterprise capacity — IdentifiFi Wireless Appliances are scalable:
 - C5110 — Up to 525 APs, 1050 APs in Controller availability mode
 - C5210 — Up to 1000 APs, 2000 APs in Controller availability mode
 - C4110 — Up to 2500 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 NetSight Suite of products. For more information, see [Extreme Networks NetSight Suite Integration](#) on page 25.

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 NetSight Suite Integration

The Extreme Networks IdentifiFi Wireless solution now integrates with the Extreme Networks NetSight Suite of products. The Extreme Networks NetSight Suite of products provides 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. For more information, see

The NetSight Suite is a family of products comprising the NetSight 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 Extreme Networks IdentifiFi Wireless solution integrates with the Automated Security Manager application, see the *Extreme Networks IdentifiFi Wireless 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 Extreme Networks IdentifiFi Wireless solution integrates with the Automated Security Manager application, see the *Extreme Networks IdentifiFi Wireless 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 Extreme Networks IdentifiFi Wireless solution integrates with the Extreme Networks NAC solution, see [NAC integration with Extreme Networks Wireless WLAN](#) on page 31.
- Policy Manager — Policy Manager recognizes the Extreme Networks IdentifiFi Wireless suite as role capable devices that accept partial configuration from Policy Manager. Currently this integration is partial in the sense that NetSight 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 IdentiFi Wireless Appliance allows Policy Manager to:

- Attach Topologies (assign VLAN to port) to the IdentiFi Wireless 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 IdentiFi Wireless Appliance ships with a default SSID, attached by default to all AP radios, when enabled.
 - Use the basic installation wizard to complete the IdentiFi Wireless Appliance configuration.
- 2 Use Policy Manager to:
 - Push the VLAN list to the IdentiFi Wireless Appliance (Topologies)
 - Attach VLANs to IdentiFi Wireless Appliance physical ports (Console - Complete Topology definition)
 - Push RADIUS server configuration to the IdentiFi Wireless Appliance
 - Push role definitions to the IdentiFi Wireless Appliance
 - Attach the default role to create a VNS
- 3 Fine tune controller settings. For example, configuring filtering at APs and IdentiFi Wireless 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.

Extreme Networks IdentiFi Wireless and Your Network

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

- IdentiFi Wireless — A rack-mountable network device that provides centralized control over all access points and manages the network assignment of wireless device clients associating through access points.
- Wireless AP — A wireless LAN fit access point that communicates with a controller.
- RADIUS Server (Remote Access Dial-In User Service) (RFC2865), or other authentication server — An authentication server that assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users in either 802.1x or Captive Portal security modes. The RADIUS Server system can be set up for certain standard attributes, such as filter ID, and for the Vendor Specific Attributes (VSAs). In addition, RADIUS Disconnect (RFC3576) which permits dynamic adjustment of user role (user disconnect) is supported.

- DHCP Server (Dynamic Host Configuration Protocol) (RFC2131) — A server that assigns dynamically IP addresses, gateways, and subnet masks. IP address assignment for clients can be done by the DHCP server internal to the controller, or by existing servers using DHCP relay. It is also used by the APs to discover the location of the controller during the initial registration process using Options 43, 60, and Option 78. Options 43 and 60 specify the vendor class identifier (VCI) and vendor specific information. Option 78 specifies the location of one or more SLP Directory Agents. For SLP, DHCP should have Option 78 enabled.
- Service Location Protocol (SLP) (SLP RFC2608) — Client applications are User Agents and services that are advertised by a Service Agent. In larger installations, a Directory Agent collects information from Service Agents and creates a central repository. The Extreme Networks solution relies on registering “Extreme Networks” as an SLP Service Agent.
- Domain Name Server (DNS) — A server used as an alternate mechanism (if present on the enterprise network) for the automatic discovery process. Controller, Access Points and Convergence Software relies on the DNS for Layer 3 deployments and for static configuration of the APs. The controller can be registered in DNS, to provide DNS assisted AP discovery. In addition, DNS can also be used for resolving RADIUS server hostnames.
- Web Authentication Server — A server that can be used for external Captive Portal and external authentication. The controller has an internal Captive portal presentation page, which allows Web authentication (Web redirection) to take place without the need for an external Captive Portal server.
- RADIUS Accounting Server (Remote Access Dial-In User Service) (RFC2866) — A server that is required if RADIUS Accounting is enabled.
- 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
 - IdentifiFi 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 Extreme Networks IdentifiFi Wireless 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.

Network Traffic Flow

Figure 3: Traffic Flow Diagram on page 28 illustrates a simple configuration with a single controller and two APs, each supporting a wireless device. A RADIUS server on the network provides authentication, and a DHCP server is used by the APs to discover the location of the controller during the initial registration process. Network inter-connectivity is provided by the infrastructure routing and switching devices.

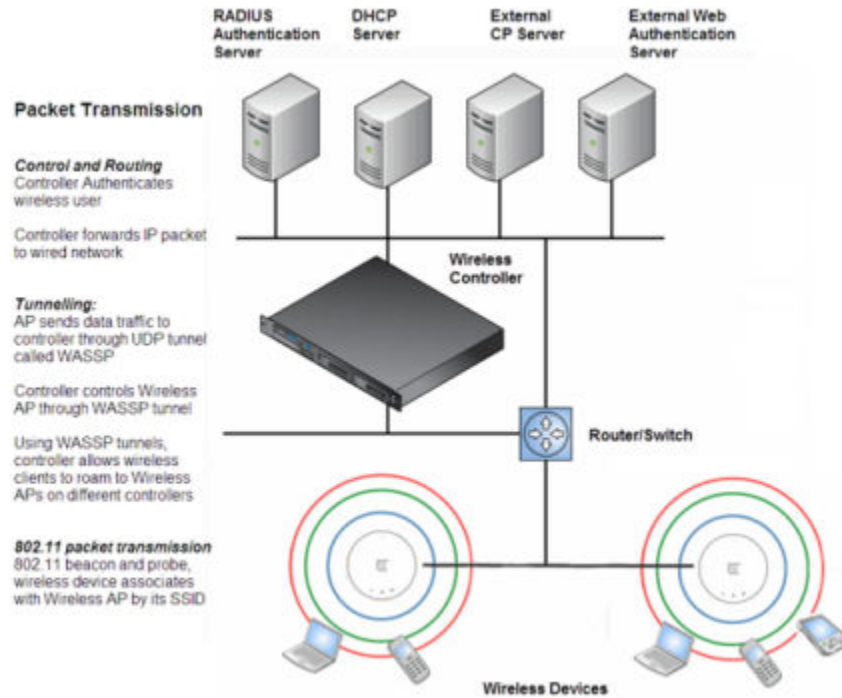


Figure 3: Traffic Flow Diagram

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

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

Network Security

The Extreme Networks IdentifiFi Wireless 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 IdentifiFi Wireless 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 IdentifiFi Wireless 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 IdentifiFi Wireless 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.

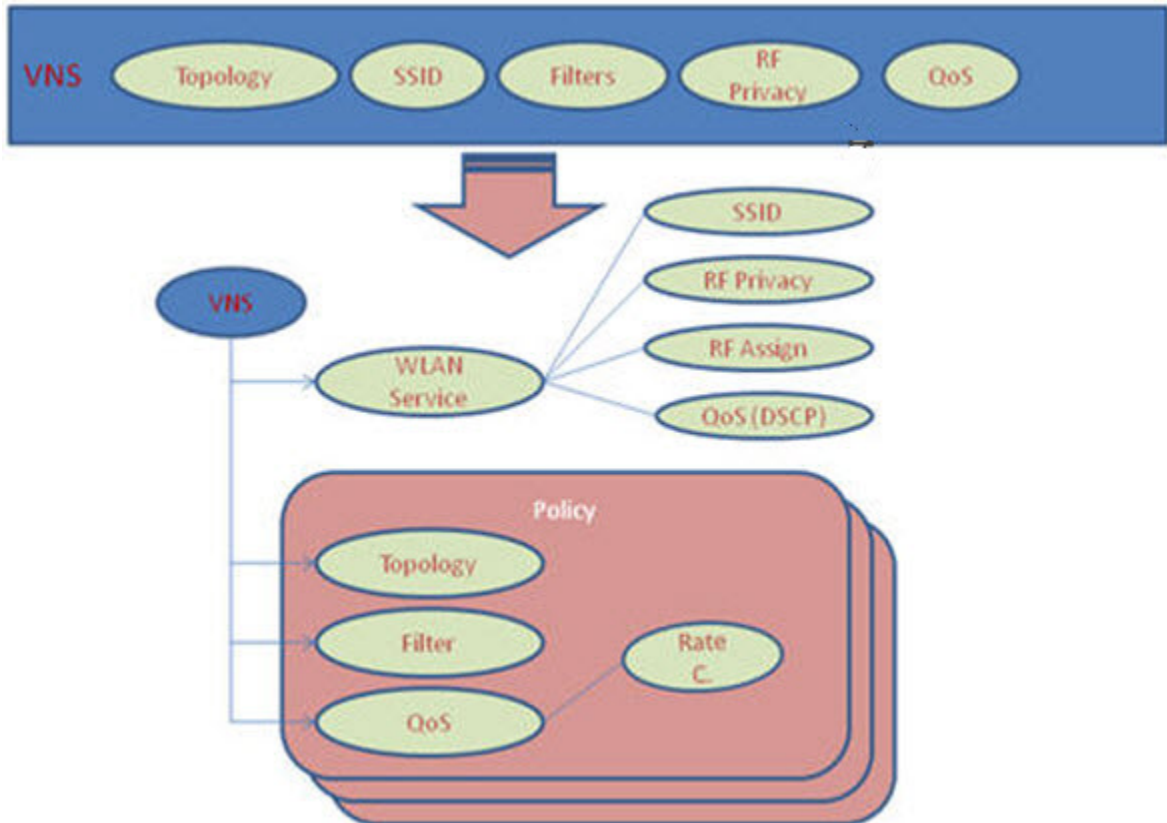


Figure 4: VNS as a Binding of Reusable Components

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 NetSight Policy Manager or NetSight Wireless Manager and pushed to the IdentifiFi Wireless Appliance. Role assignment ensures that the correct topology and traffic behavior are applied to a user regardless of WLAN service used or VNS assignment.

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

If the OSPF 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 specified number of active VNSs, as listed below:

- C5110 — Up to 128 VNSs
- C5210 — Up to 128 VNSs
- C4110 — Up to 64 VNSs
- C25 — Up to 16 VNSs
- C35 — Up to 48 VNSs
- V2110 Small — Up to 16 VNSs
- V2110 Medium — Up to 64 VNSs
- V2110 Large — Up to 128 VNSs

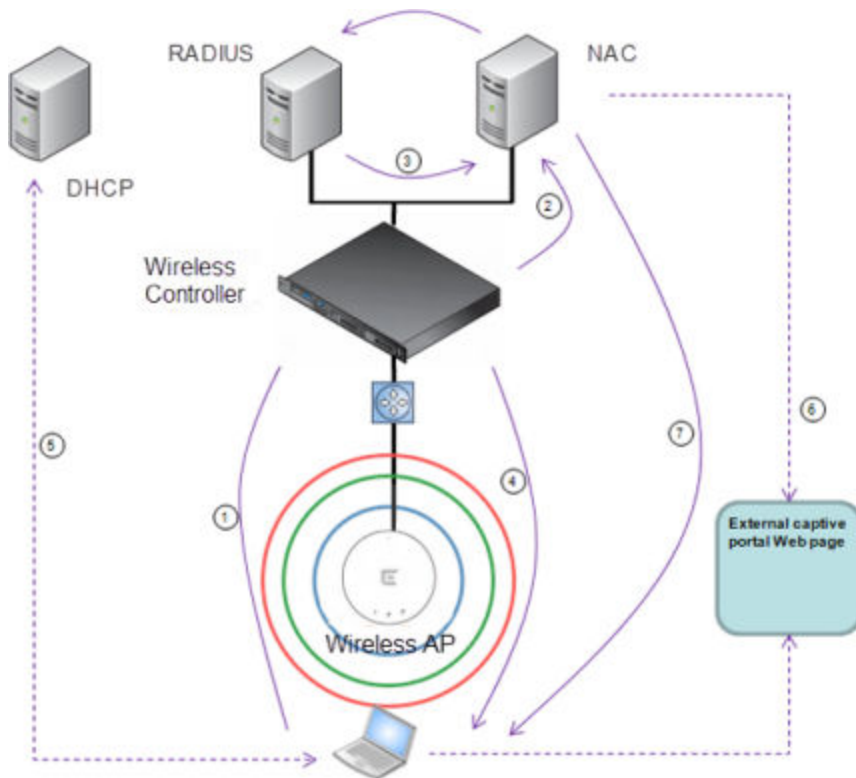
The AP radios can be assigned to each of the configured WLAN services and, therefore, VNSs in a system. Each AP can be the subject of 16 service assignments—eight assignments per radio—which corresponds to the number of SSIDs it can support. Once a radio has all eight slots assigned, it is no longer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

NAC integration with Extreme Networks Wireless WLAN

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 Extreme Networks Wireless WLAN supports SSID VNSs when used in conjunction with MAC-based external captive portal authentication.

[Figure 5: WLAN and NAC Integration with External Captive Portal Authentication](#) on page 32 depicts the topology and workflow relationship between Extreme Networks 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 317.



- 1 The client laptop connects to the AP.

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

- 2 The Identifi Wireless 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.

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 Identifi Wireless Appliance and Identifi Wireless AP.

- 4 The Identifi Wireless Appliance and Identifi Wireless AP apply role against the client laptop accordingly. The Identifi Wireless Appliance assigns a set of filters to the client laptop's session and the Identifi Wireless AP allows the client laptop access to the network.

- 5 The client laptop interacts with a DHCP server to obtain an IP address.

- 6 Eventually the client laptop uses its Web browser to access a Website.

- The Identifi Wireless Appliance determines that the target Website is blocked and that the client laptop still requires authentication.
- The Identifi Wireless 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 IdentifiFi Wireless Appliance.

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

The IdentifiFi Wireless Appliance forwards the command to terminate the client laptop's session to the IdentifiFi Wireless 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.

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, Class of Service (CoS) refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a 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 IdentifiFi Wireless 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.
- 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.

As of Release V7.0, the components of a WLAN Service map to the corresponding components of a VNS in previous releases. The exception is that WLAN Services are not classified as SSID-based or AAA-based, as was the case in previous releases. Instead, the administrator makes an explicit choice of the type of authentication to use on the WLAN Service. If his choice of authentication option conflicts with any of his 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 IdentifiFi Wireless 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 IdentifiFi Wireless 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 IdentifiFi Wireless 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 IdentifiFi Wireless 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)

IdentifiFi Wireless Appliance Product Family

The IdentifiFi Wireless Appliance is available in the following product families:

Table 3: IdentifiFi Wireless Appliance Product Families

IdentifiFi Wireless 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 IdentiFi Wireless Appliance

System Configuration Overview
Logging on to the IdentiFi Wireless Appliance
Wireless Assistant Home Screen
Working with the Basic Installation Wizard
Configuring the IdentiFi Wireless Appliance for the First Time
Using an AeroScout/Ekahau 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 your system:

- 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 DHCP 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.
 - Create a new physical topology and provide the IP address to be the relevant subnet point of attachment to the existing network.
 - To manage the controller through the interface configured above, select the Mgmt checkbox on the **Interfaces** tab.
 - 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.
 - 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 91.

- 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 Identifi Wireless 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 Identifi Wireless Appliance from changing the licensed region, and in addition, manually configured channel settings will be maintained. For more information, see the Extreme Networks Identifi Wireless *Maintenance Guide*.

- 5 Configure the controller for remote access:
 - 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.
 - Configure the controller's management interface.
 - Configure the data interfaces.
 - Set up the controller on the network by configuring the physical data ports.
 - Configure the routing table.
 - Configure static routes or OSPF parameters, if appropriate to the network.

For more information, see [Configuring the Identifi Wireless Appliance for the First Time](#) on page 51.

- 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 212.
- 7 Configure roles. Roles are typically bound to topologies. Role application assigns user traffic to the corresponding network point.
 - Roles define user access rights (filtering or ACL)
 - Policies reference user's rate control profile.

For more information, see [Configuring Roles](#) on page 228.

- 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 243.

- 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.

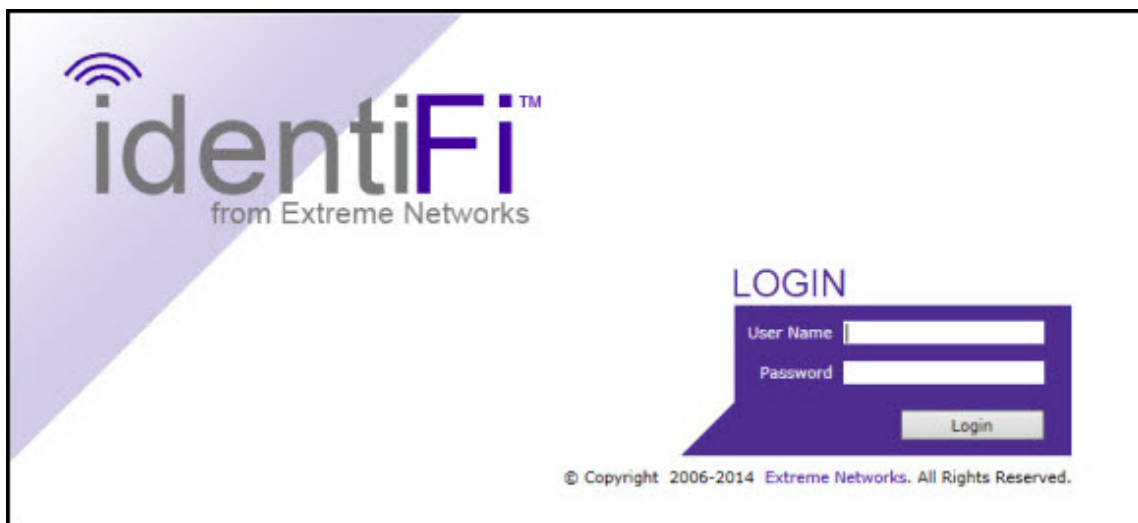
- Confirm the latest firmware version is loaded. For more information, see [Performing AP Software Maintenance](#) on page 181.
- Deploy APs to their corresponding network locations.
- If applicable, configure a default AP template for common radio assignment, whereby APs automatically receive complete 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 Identifi Wireless APs](#) on page 100.
- 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 Identifi Wireless Appliance

- 1 Launch your Web browser (Internet Explorer version 6.0 or higher, or FireFox).
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.



- In the **User Name** box, type your user name.
- In the **Password** box, type your password.



Note

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

- Click **Login**. The Wireless Assistant Home screen displays.

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 (Network Status, Admin sessions, and so on) and provides a graphical representation of active AP information (such as the number of wired packets, stations, and total APs).

The top menu bar displays across each page within the Wireless Assistant. Using the top menu bar, you can access controller's APs, VNS Configurations, Radar, and online help. [Figure 6: Wireless Assistant Top Menu Bar](#) on page 41 shows the Wireless Assistant top menu bar.

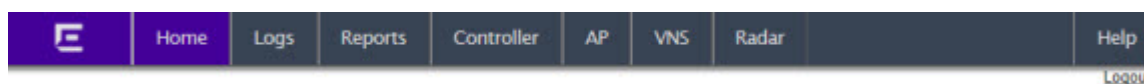


Figure 6: Wireless Assistant Top Menu Bar

The bottom status bar displays across the bottom of each page within the Wireless Assistant. Viewing the bottom status bar, you can see 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 Bottom Status Bar](#) on page 42 shows the Wireless Assistant bottom status bar.



Figure 7: Wireless Assistant Bottom Status Bar

Figure 8: Wireless Assistant Home Screen on page 42 shows the Wireless Assistant Home Screen.
 Table 4: Wireless Assistant Home Screen Headings on page 43, describes the home screen headings and descriptions with links to support information within the User Guide.

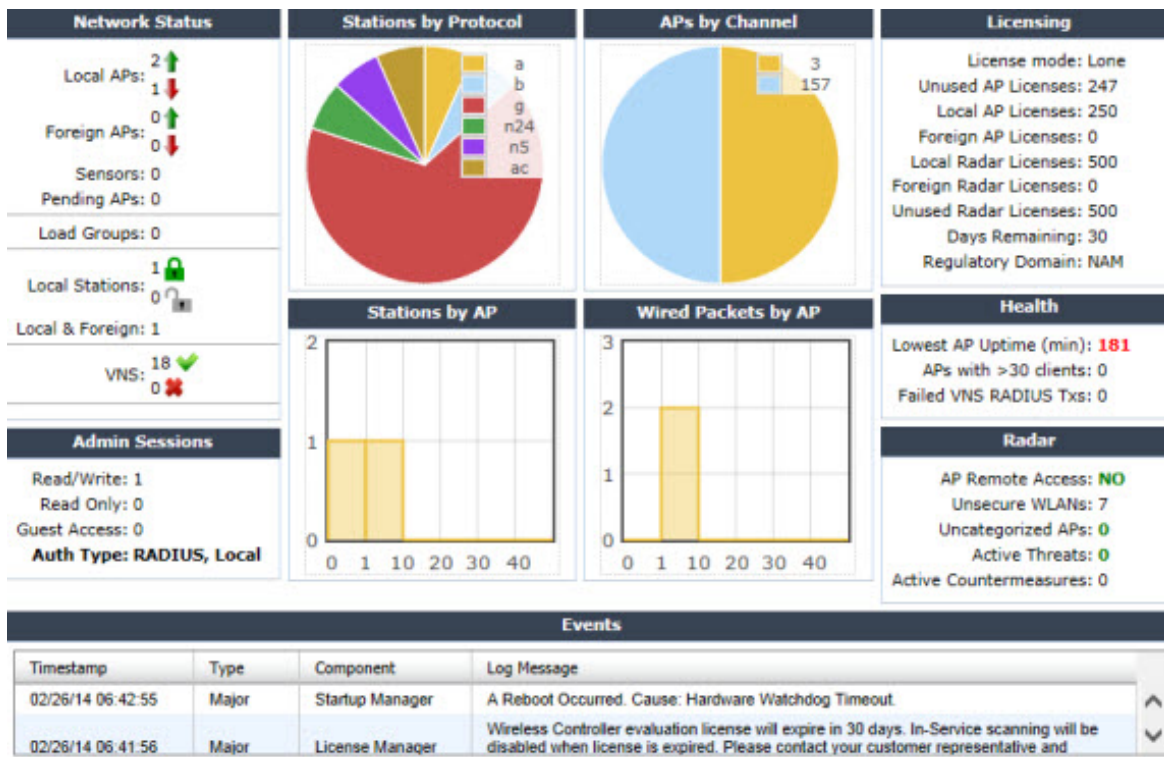


Figure 8: Wireless Assistant Home Screen

Table 4: Wireless Assistant Home Screen Headings

Home Screen Heading	Description
Network Status	<p>Includes real-time totals for the following components:</p> <ul style="list-style-type: none"> • Local APs - total number of active or inactive local configured APs. Click the number displayed to open a separate dialog that lists the AP name, serial number, tunnel info, and IP address. • Foreign APs - total number of active or inactive foreign configured APs. Click the number displayed to open a separate dialog that lists the AP name, serial number, IP address, and tunnel info for active APs (if availability pair is configured). • Sensors - total number of active sensors. Click the number displayed to open a separate dialog that lists the sensor name, serial number, and IP address. • Pending APs - total APs pending verification. Click the number displayed to open a separate dialog that lists the AP name, serial number, and IP address. • Load Groups - total active load groups. Click Load Groups to display the Active Wireless Load Groups report. • Local Stations - total number of active mobile stations. Click Local Stations to display the All Active Client report. • Local & Foreign - total number of active and foreign stations. Click Local & Foreign to display the All Active Client report. • VNS - total defined VNSs (enabled and disabled). Click VNS to display the total number of enabled and disabled VNS assignments, respectively, configured on the system. • Availability - status of the controller availability. Click Availability to display controller settings (Stand-alone, Paired, Fast Failover FFO). • Mobility Tunnels - status of the mobility tunnel. Click Mobility 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 78.</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 505.</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 505.</p>

Table 4: Wireless Assistant Home Screen Headings (continued)

Home Screen Heading	Description
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 505.</p>
Wired Packets by AP	<p>Displays a graphical representation of packet statistics including the total number of packets sent and received, the total packets discarded, and the total number of unicast, multicast, and broadcast packets.</p> <p>Click the Wired Packets by AP heading to access the Wireless Status by Wireless AP Report. For more information, see Viewing Statistics for APs on page 505.</p>
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 License Manger startup and 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 or 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 52). 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 458). 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 54.</p>
Health	<p>Displays network health statistics including:</p> <ul style="list-style-type: none"> Local AP Uptime (min) APs with > 30 clients 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 505.</p>

Table 4: Wireless Assistant Home Screen Headings (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 <p>For more information, see Defining Properties for the Discovery Process on page 115, and Working with Radar Reports on page 493.</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 Logs > Logs & Traces page. For more information, see Available Reports and Statistics on page 504.</p>

Working with the Basic Installation Wizard

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

Administrators can use the basic installation wizard to quickly configure the controller for deployment, and then once the installation is complete, continue to revise the controller configuration accordingly.

The basic installation wizard is automatically launched when an administrator logs on to the controller for the first time, including when the system has been reset to the factory default settings. In addition, the basic installation wizard can also be launched at any time from the left pane of the controller Configuration screen.

To configure the controller with the Basic Installation Wizard:

- 1 Log on to the controller. For more information, see [Logging on to the Identifi Wireless Appliance](#) on page 40.
- 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** — Click the appropriate large-scale geographic grouping for the time zone.
 - **Country** — Click the appropriate country for the time zone. The contents of the drop-down list change, based on the selection in the **Continent or Ocean** drop-down list.
 - **Time Zone Region** — Select the appropriate time zone region for the selected country from the drop-down menu.
- 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 **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.

- 2 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.
- 3 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.
- 4 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.

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

Basic Installation Wizard - Services Screen

The **Services** screen displays:

- 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 Identifi Wireless 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 Identifi Wireless Appliance is configured as a mobility manager, the Identifi Wireless Appliance's 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 448.
 - **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. The default VNS parameters are displayed.
Refer to [Virtual Network Services](#) on page 29 for more information about the default VNS.
- 5 Click **Finish**. The **Success** screen displays

Basic Installation Wizard - Success Screen

- 1 We recommend that you change the factory default administrator password. To do so:
 - 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.
- 2 Click **OK**, and then click **Close**. The IdentifiFi Wireless Assistant home screen displays.

Note



The IdentifiFi Wireless 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 IdentifiFi Wireless Assistant session is terminated and you will need to log back in with the new IP address.

Success! ✓

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

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

New Password:

Confirm Password:

Save

Back Close

Configuring the IdentiFi Wireless Appliance for the First Time

As soon as the IdentiFi Wireless Appliance is deployed, you should perform a series of configuration tasks. These tasks include:

- [Changing the Administrator Password](#) on page 51
- [Applying Product License Keys](#) on page 52
- [Setting Up the Data Ports](#) on page 56
- [Setting Up Internal VLAN ID and Multicast Support](#) on page 63
- [Setting Up Static Routes](#) on page 64
- [Setting Up OSPF Routing](#) on page 66
- [Configuring Filtering at the Interface Level](#) on page 69
- [Protecting the Controller's Interfaces and Internal Captive Portal Page](#) on page 72
- [Configuring the Login Authentication Mode](#) on page 78
- [Configuring SNMP](#) on page 88
- [Configuring Network Time](#) on page 91
- [Configuring DNS Servers for Resolving Host Names of NTP and RADIUS Servers](#) on page 95

Although the basic installation wizard has already configured some aspects of the controller deployment, you can continue to revise the controller configuration according to your network needs.

Changing the Administrator Password

Extreme Networks recommends that you change your default administrator password once your system is deployed. The IdentiFi Wireless 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**. The screen displays.
- 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 IdentiFi Wireless 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 78.

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 V9.01 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 IdentiFi Wireless Appliance's limit. Depending on the IdentiFi Wireless 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 25 wireless APs

V2110 — Adds 1 or 16 wireless APs

**Note**

If you connect additional wireless APs to an IdentiFi Wireless 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 458). 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 5: 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	25	125	4 to 34 (depending on the enhancement license type used)
C4110	50	250	8
C5110	150	525	15
C5210	100	1000	9 to 36 (depending on the enhancement license type used)
V2110	8	525	17 to 242 (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 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 430).

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 IdentifiFi Wireless License Certificate, which is sent to you via traditional mail.

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

To Install the License Keys:

- 1 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Administration** > **Software Maintenance**.

- 3 Click the **EWC Product Keys** tab.

The bottom pane displays the license summary.

The screenshot shows the 'EWC Product Keys' configuration page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar lists 'Administration' options: Availability, Flash, Host Attributes, Installation Wizard, Login Management, Software Maintenance, System Maintenance, and Web Settings. Below the sidebar are sections for 'Logs', 'Network', and 'Services'. The main content area has tabs for 'EWC Software', 'Backup', 'Restore', and 'EWC Product Keys'. Under 'EWC Product Keys', there are two input fields: 'Activation Key' and 'Option Key', each with an 'Apply' button. The 'Activation Key' field has a format: 'AAAAAA-11111111-11111111-11111111-11111111'. The 'Option Key' field has a format: 'Capacity Enhancement Key Format: For AP: CAPxxx-11111111-11111111-11111111-11111111 For Radar: RADCAPxxx-11111111-11111111-11111111-11111111'. A red error message '*Option Key limit reached.' is displayed below the Option Key field. Below the input fields is a 'License Summary' section with the following details: Locking ID: 84-2B-2B-70-B9-4D, Regulatory Domain: North America, Number of Licensed APs: 250, Number of Licensed APs for Radar: 500, and Evaluation period: 30 day(s) left in this 30-day evaluation period. A 'View Installed Keys' button is located at the bottom right of the License Summary section.

- 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: TRDKNAM-R22KK2YV-4ZYXL00I-QF9QX1YR-XYBUUD5I

Licensed Software Release: 09.01.01.0202

Regulatory Domain: North America

Option Keys:

Feature	License Key	Description

Licensed AP Totals:

Base Number of APs:	250
Option Number of APs:	-
<hr/>	
Total Licensed APs:	250

APs Licensed for Radar:

Base Number of APs licensed for Radar:	500
Option Number of APs licensed for Radar:	-
<hr/>	
Total Licensed APs for Radar:	500

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 Identifi Wireless 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 57.

Link Aggregation ports are represented by the L2 (peer-to-peer) LAG Ports. The L2 port and Topology information can be accessed from **L2 Ports** and **Topology** tabs under Identifi Wireless 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 57.



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 58 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**. The screen displays.
- 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 Link Aggregation LAG (peer to peer) data ports that exist on the controller. These ports cannot be deleted and new ones cannot be created.

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

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

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

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

Physical:

- C5110 — Three data ports, displayed as esa0, esa1, and esa2.
- C5210 — Four data ports, displayed as esa0, esa1, esa2, and esa3.
- 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 — One data port, displayed as lag1.
 - 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 210.

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 58 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**. The screen displays.
- 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 of topology entries. Below the table are buttons for 'New' and 'Delete Selected', and configuration fields for 'Internal VLAN ID' (set to 1) and 'Multicast Support' (set to Port1). A 'Save' button is located at the bottom right.

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:

- 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 Identifi Wireless 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 (v2, V3, get), SSH, and HTTPs management interfaces.

Note



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

- 11 To enable the local DHCP Server on the controller, in the **DHCP** 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**. The screen displays.
- 2 In the left pane, click **Network > Topologies**. The **Topologies** tab is displayed.

The screenshot shows the 'Topologies' configuration page in the Identifi Wireless Controller. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar shows 'Administration', 'Logs', 'Network', 'L2 Ports', 'Network Time', 'Routing Protocols', 'Secure Connections', 'SNMP', 'Topologies', and 'Utilities'. 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'. 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 'Wireless Controller Configuration' interface. 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 contains a tree view with 'Administration', 'Logs', 'Network' (selected), 'L2 Ports', 'Network Time', 'Routing Protocols', 'Secure Connections', 'SNMP', 'Topologies', and 'Utilities'. The main content area has tabs for 'View Forwarding Table', 'Static Routes' (selected), and 'OSPF'. Below the tabs 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 56).

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**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Network** > **Routing Protocols**. The **Static Routes** tab is displayed by default.
- 3 Click the **OSPF** tab.

The screenshot displays the OSPF configuration page. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar shows a tree view with Administration, Logs, Network (selected), and Services. Under Network, there are sub-items: L2 Ports, Network Time, Routing Protocols (selected), Secure Connections, SNMP, Topologies, and Utilities. The main content area is titled 'View Forwarding Table' and has tabs for 'Static Routes' and 'OSPF'. The 'OSPF' tab is active, showing 'Global Settings' and 'Interface Settings'. The 'Global Settings' section includes 'OSPF Status' (set to 'On'), 'Area id' (0.0.0.2), 'Router id' (empty), and 'Area Type' (Default). A 'Save' button is present. The 'Interface Settings' section is a table with columns: Topology, Enabled, Authentication, Password, Cost, H/I, D/I, RT/I, and Delay. It lists four ports: Port1 (Enabled), Port2 (Disabled), Port3 (Disabled), and Port4 (Disabled). 'New' and 'Delete Selected' buttons are at the bottom.

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

- 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.

- 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 230.

- 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 IdentiFi Wireless 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**. The **Wireless Controller Configuration** screen displays.
- 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

Internal VLAN ID:
 Multicast Support:

- 3 On the **Topologies** tab, click the appropriate data port topology. The Edit Topology window displays.
- 4 Select the **Management Traffic** 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 230.

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).

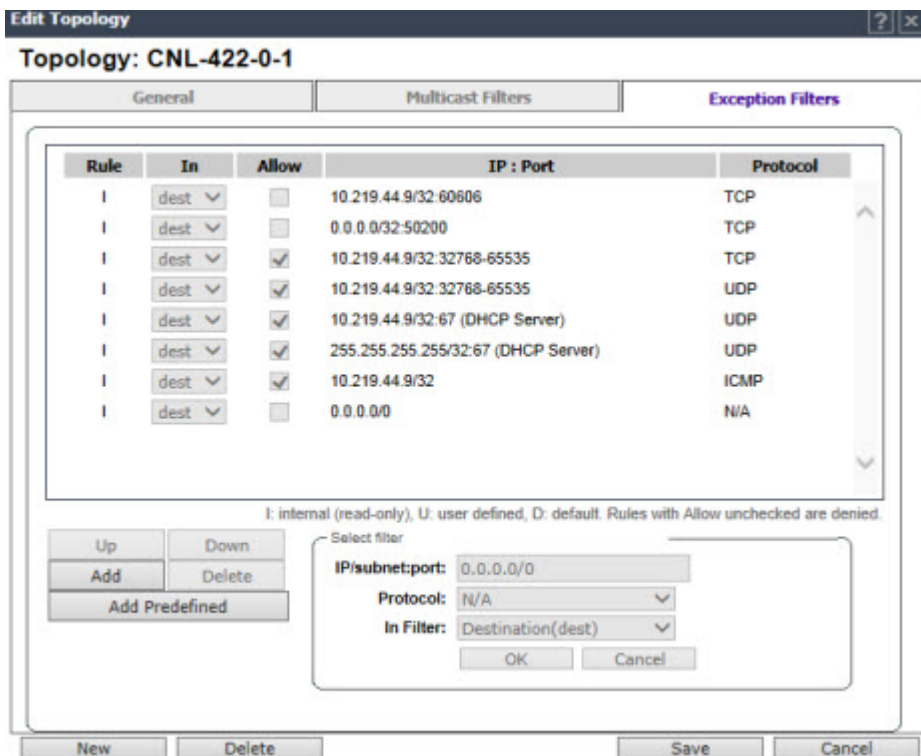


Warning

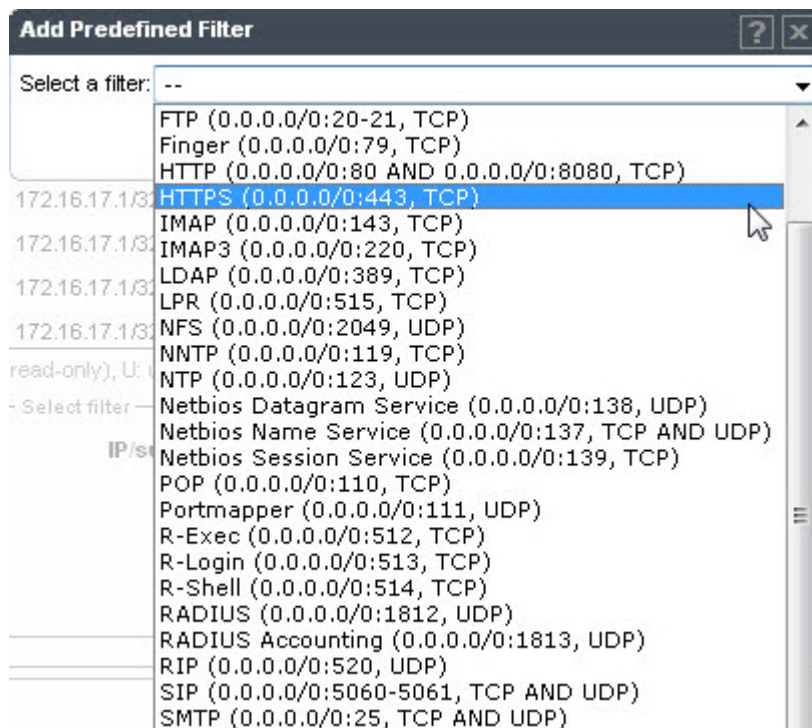
If defined improperly, user exception rules may seriously compromise the system's normal security enforcement rules. They may also disrupt the system's normal operation and even prevent system functionality altogether. It is advised to only augment the exception-filtering mechanism if absolutely necessary.

To Define Interface Exception Filters:

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



- 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, ICMP. 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 6: Supported Certificate and CA Formats](#) on page 73.

Table 6: 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 Identifi Wireless *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

You can install a certificate from the Certificates tab available on the Topologies page.

To Install a Certificate for a Controller Data Interface:

- 1 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
- 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 7: Topologies Page: Certificates Tab Fields and Buttons](#) on page 74 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 7: Topologies Page: Certificates Tab Fields and Buttons

Field/Button	Description
Interface Certificates	
Topology	Topology name

Table 7: Topologies Page: Certificates Tab Fields and Buttons (continued)

Field/Button	Description
Expiry Date	Date when the certificate expires
CA Cert.	Identifies whether or not a CA certificate has been installed on the topology.
Name (CN)	The IP address of DNS address associated with the topology that the certificate applies to. Note: The Name field supports both IPv4 or IPv6 addresses.
Org Unit (OU)	Name of the organization's unit.
Organization	Name of the organization
Configuration for Topology	
Replace/Install selected Topology's certificate	<p>To replace/install the existing port's certificate and key using this option, do the following:</p> <ol style="list-style-type: none"> 1 From the click the Generate Signing Request button to create the certificate and key. 2 Download the CSR when prompted. 3 Use a 3rd party certificate service to sign the CSR and create a certificate and a Certificate Authority (CA) file. 4 Save the certificate on your computer. 5 Return to the Certificates tab on the IdentiFi Wireless Assistant 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 7: 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 7: 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 9: Generate Certificate Signing Request Window on page 77)
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 9: Generate Certificate Signing Request Window

Table 8: 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 8: 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 78.
- RADIUS authentication — The controller uses login credentials and passwords configured on a RADIUS server. See [Configuring the RADIUS Login Authentication Mode](#) on page 80.
- 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 84.
- 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 86.



Note

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

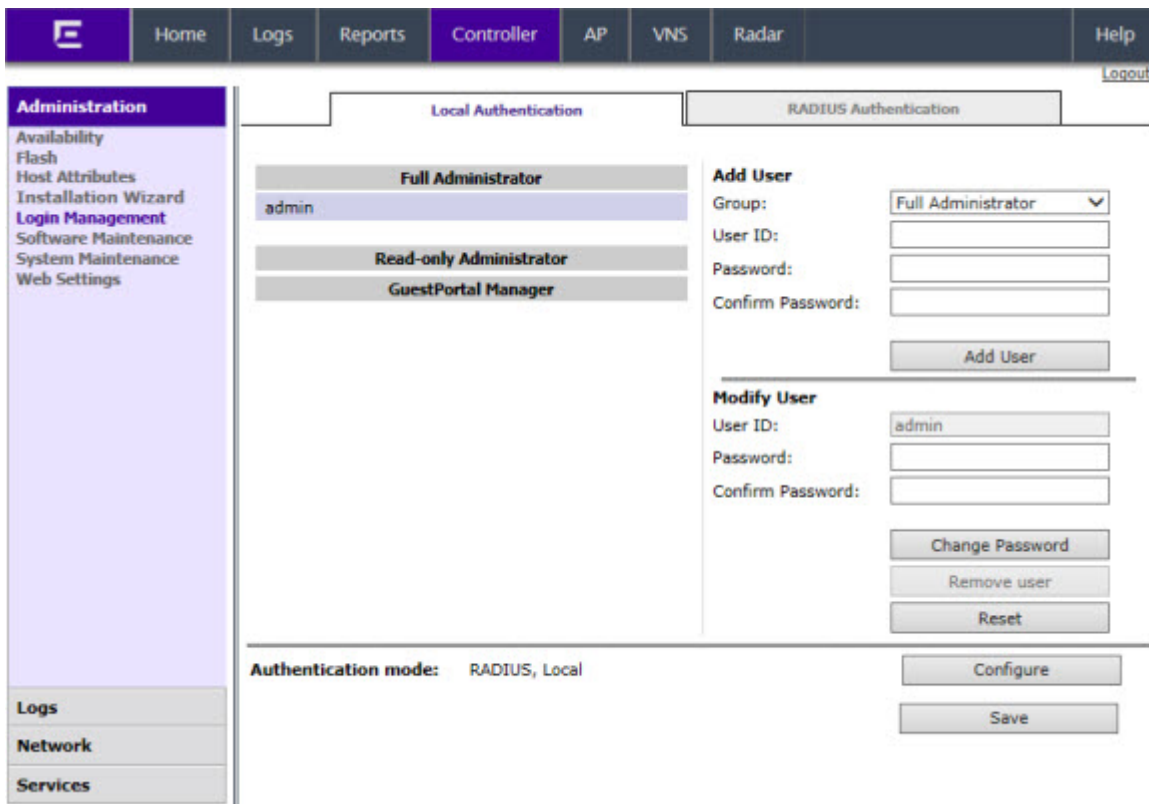
Configuring the Local Login Authentication Mode and Adding New Users

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 549.

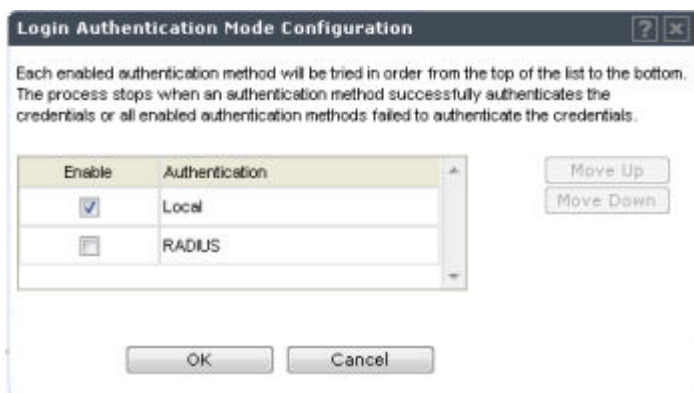
To configure the local login authentication mode:

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

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



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



- Select the **Local** checkbox.
If the RADIUS checkbox is selected, deselect it.
- OK**
- 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 292.

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.

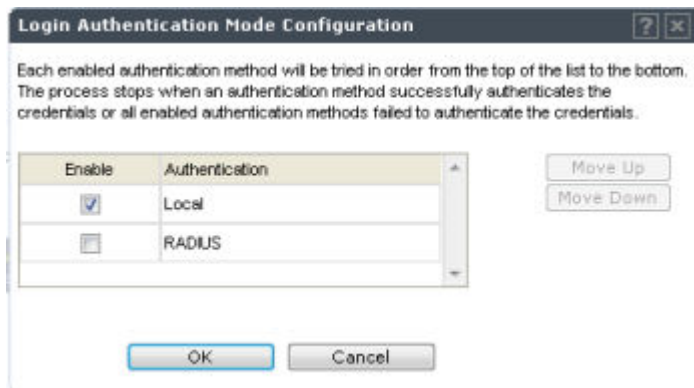
To configure the RADIUS login authentication mode:

- 1 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Administration** > **Login Management**. The **Login Management** screen displays.
- 3 Click the **RADIUS Authentication** tab.

The screenshot shows the 'Controller' configuration page with the 'RADIUS Authentication' tab selected. The interface includes a top navigation bar with 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. A left sidebar lists 'Administration' options: 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 has two tabs: 'Local Authentication' and 'RADIUS Authentication'. Under 'RADIUS Authentication', there is a 'Configured Servers' section with a table containing one entry: 'Smoke Test Radius Ser'. To the right of this table is an 'Auth +' section with a checked box for 'Use server for Authentication'. Below this are fields for 'NAS IP Address' (10.219.40.1), 'NAS identifier' (lab-422-g), and 'Auth. type' (CHAP). A 'Reset' button is located below these fields. 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 292.

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.

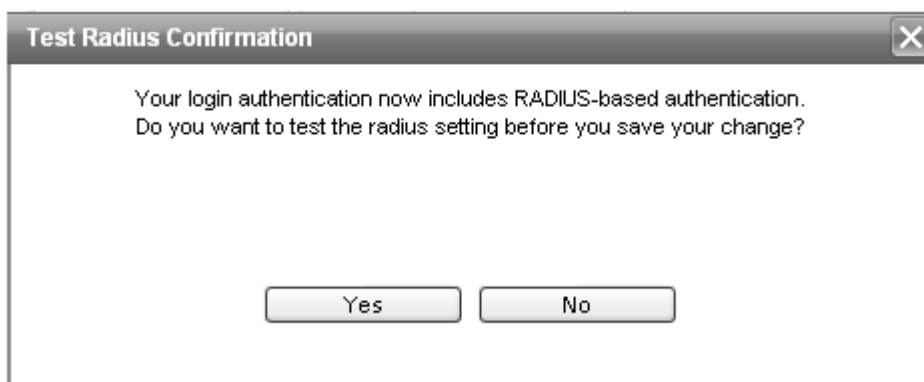
The screenshot shows the same "Test RADIUS Servers" dialog box, but now it displays the results. The text "RADIUS Test Results:" is followed by "Successful". A "Close" button is centered at the bottom of the dialog.

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.

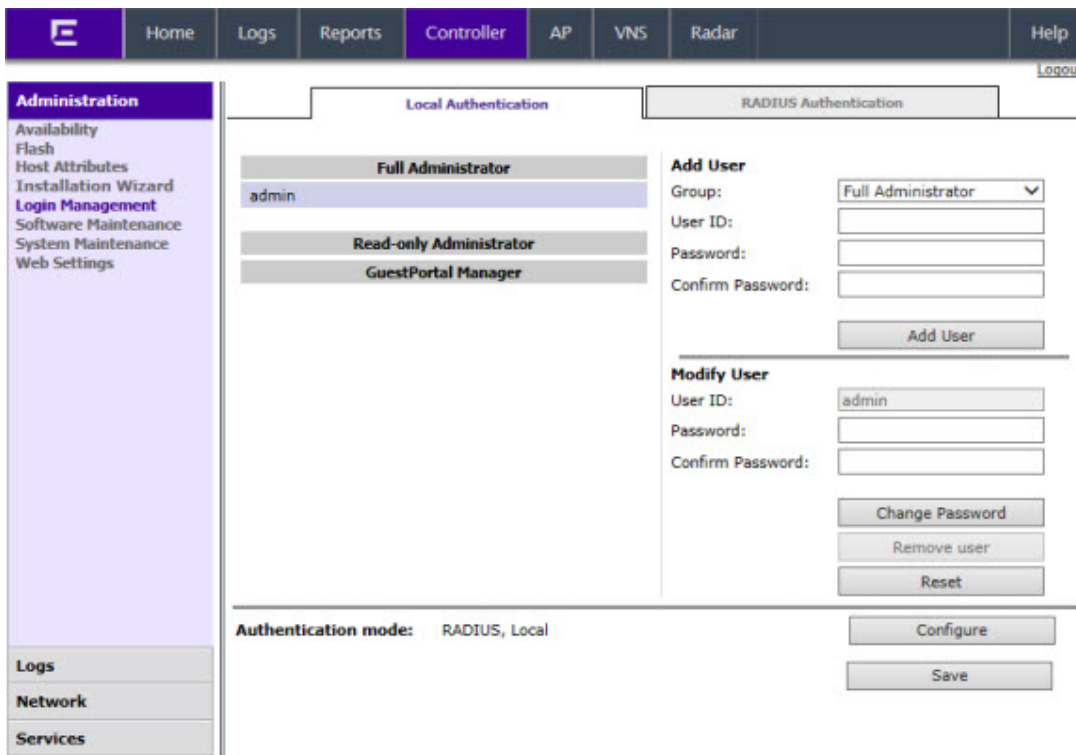
To cancel the authentication mode changes, click **Cancel**.

Configuring the Local, RADIUS Login Authentication Mode

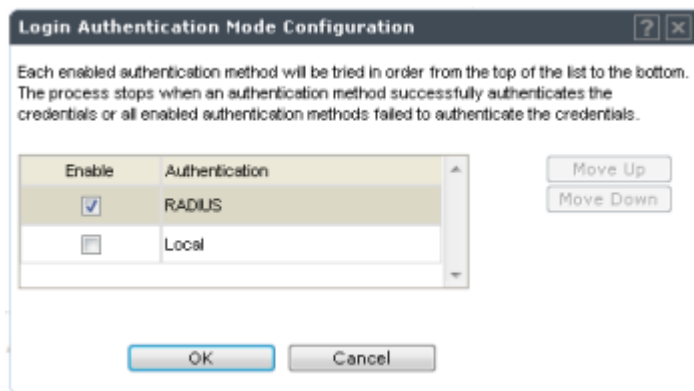
To configure the Local, RADIUS login authentication mode:

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

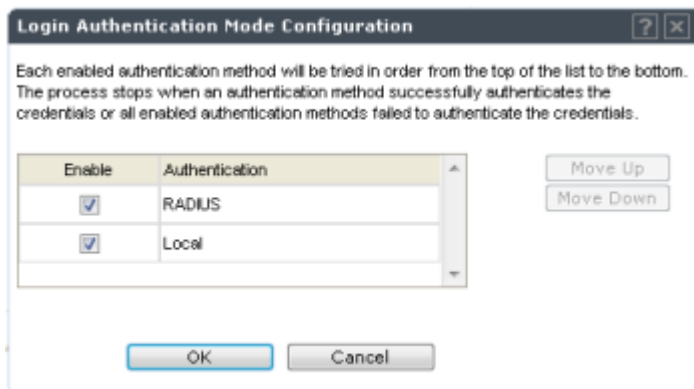
- In the left pane, click **Administration** > **Login Management**. The **Login Management** screen displays.



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



- 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 78.

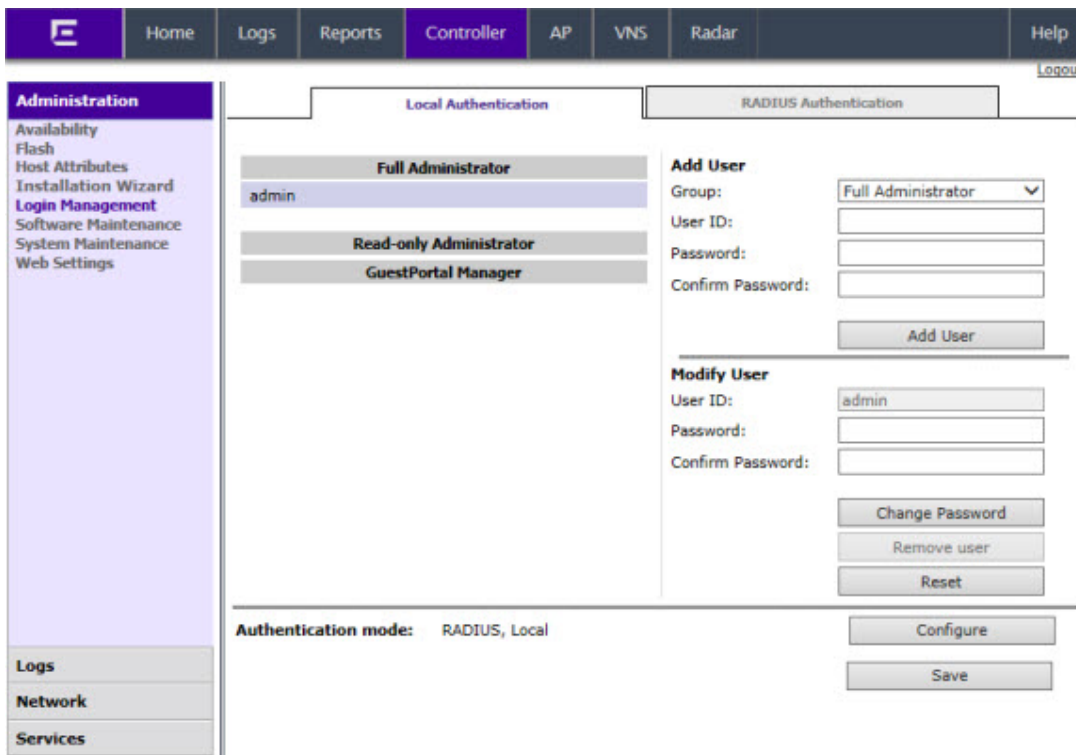
For information on setting RADIUS login authentication settings, see [Configuring the RADIUS Login Authentication Mode](#) on page 80.

Configuring the RADIUS, Local Login Authentication Mode

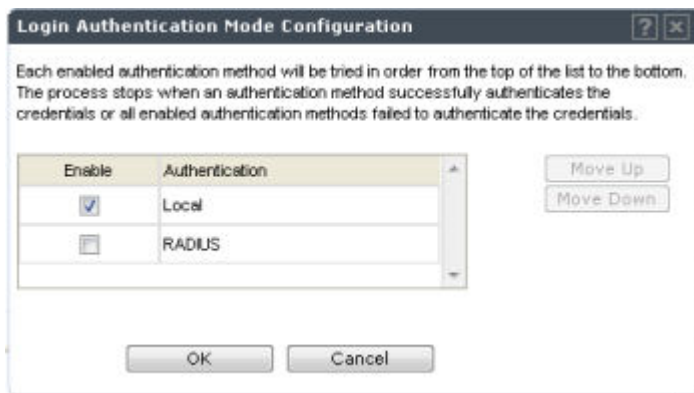
To configure the RADIUS, Local login authentication mode:

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

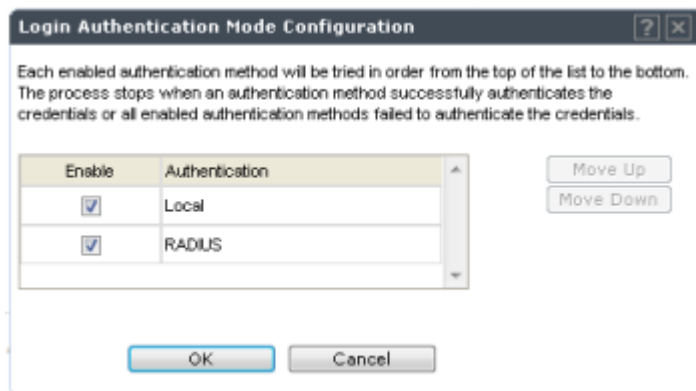
- In the left pane, click **Administration > Login Management**. The **Login Management** screen displays.



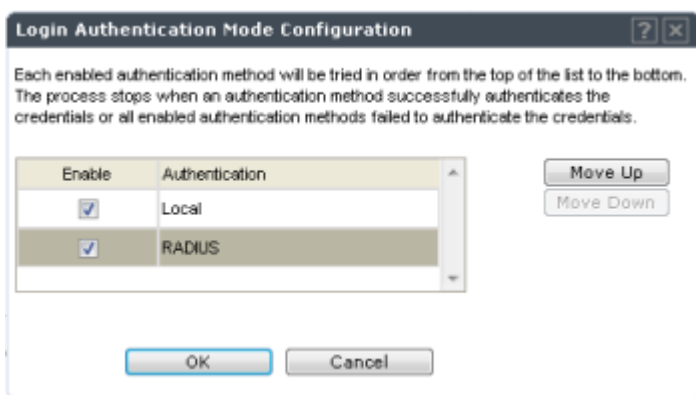
- In the **Authentication mode** section, click **Configure**. The **Login Authentication Mode Configuration** window is displayed.



- 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 80.

For information on setting local login authentication settings, see [Configuring the Local Login Authentication Mode and Adding New Users](#) on page 78.

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 shows the web interface for configuring SNMP. The left sidebar has a menu with 'Administration', 'Logs', 'Network', 'L2 Ports', 'Network Time', 'Routing Protocols', 'Secure Connections', 'SNMP', 'Topologies', and 'Utilities'. The 'Network' menu is expanded to show 'SNMP'. The main area is titled 'SNMP Common Settings' and contains the following configuration options:

- Mode:** Radio buttons for No SNMP, **SNMPv1/v2c** (selected), 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' (active) and 'SNMPv3'. The 'SNMPv1/v2c' tab contains:

- 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 Continue with the appropriate procedure for configuring SNMPv1/v2c-specific or SNMPv3-specific parameters.
- [Configuring SNMPv1/v2c-specific Parameters](#) on page 90
 - [Configuring SNMPv3-specific Parameters](#) on page 90

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: MD5, 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**. The **Wireless Controller Configuration** screen displays.
- 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**. The **Wireless Controller Configuration** screen displays.
- 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**.

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 504.

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

The screenshot shows the 'Network Time' 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 'Network Time' and contains the following sections:

- Time Zone Settings***:
 - Continent or Ocean: Americas (dropdown)
 - Country: Canada (dropdown)
 - Time Zone Region: Eastern Time - Ontario & Quebec - most locations (dropdown)
 - TZ = America/Montreal
 - Apply Time Zone button
 - *Time Zone changes may take up to 60 seconds to take effect
- System Time**: 02-27-2014 10:18 (mm-dd-yyyy hh:mm) Set Clock button
- NTP** (checked):
 - Time Server 1: 192.168.3.100
 - Time Server 2: (empty)
 - Time Server 3: (empty)
 - Run local NTP Server checkbox (unchecked)
 - 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 **Country** drop-down list, click the appropriate country for the time zone. The contents of the drop-down list change, based on the selection in the **Continent or Ocean** drop-down list.
- 5 From the **Time Zone Region** drop-down list, click the appropriate time zone region for the selected country.
- 6 Click **Apply Time Zone**.
- 7 In the **System Time** box, type the system time.
- 8 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:

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

- 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***: Three dropdown menus for 'Continent or Ocean' (Americas), 'Country' (Canada), and 'Time Zone Region' (Eastern Time - Ontario & Quebec - most locations). Below these is a summary 'TZ = America/Montreal' and an 'Apply Time Zone' button. A red note states: '*Time Zone changes may take up to 60 seconds to take effect'.
- System Time**: A text box containing '02-27-2014 10:18' and a 'Set Clock' button.
- NTP**: A checked checkbox labeled 'NTP'. Below it are three text boxes for 'Time Server 1' (192.168.3.100), 'Time Server 2', and 'Time Server 3'. There is an unchecked checkbox for 'Run local NTP Server' and an '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 **Country** drop-down list, click the appropriate country for the time zone. The contents of the drop-down list change, based on the selection in the **Continent or Ocean** drop-down list.
- 5 From the **Time Zone Region** drop-down list, click the appropriate time zone region for the selected country.
- 6 Click **Apply Time Zone**.
- 7 In the **System Time** box, type the system time.
- 8 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 then skip to 11 on page 93.

- 9 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.

- 10 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.
- 11 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**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Network** > **Secure Connections**. The **Secure Connections** screen displays.

The screenshot shows the 'Secure Connections' configuration page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar has 'Administration', 'Logs', 'Network', 'L2 Ports', 'Network Time', 'Routing Protocols', 'Secure Connections', 'SNMP', 'Topologies', and 'Utilities'. The main content area is titled 'Shared Secret for Remote Connections' and contains a checked checkbox for 'Enable Weak Ciphers'. Below this is a table with two columns: 'Peer IP Address' and 'Shared Secret'. At the bottom, there are input fields for a new entry, an 'Add / Update' button, and a 'Save' button.

- 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

Since the **Global Settings** screen (top menu > **VNS** > Global Settings) 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.

**Note**

For more information on RADIUS server configuration, see [Defining RADIUS Servers and MAC Address Format](#) on page 293.

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**. The **Wireless Controller Configuration** screen displays.

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

The screenshot shows the 'Host Attributes' configuration page. The top navigation bar includes Home, Logs, Reports, Controller (selected), AP, VNS, Radar, and Help. The left sidebar shows 'Administration' with sub-items: Availability, Flash, Host Attributes (selected), Installation Wizard, Login Management, Software Maintenance, System Maintenance, and Web Settings. Below the sidebar are sections for Logs, Network, and Services. The main content area is titled 'Host Attributes' and contains three sections: 'Network Identification' with fields for 'Host Name' (EWC) and 'Domain Name' (enterasys.com); 'DNS' with a list of servers (empty), a 'Server Address' field, an 'Add Server' button, and 'Remove selected server' and 'Move up' buttons; and 'Default Gateway IP' with a field containing 192.168.3.7. A 'Save' button is located at the bottom right of the form.

- 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 an AeroScout/Ekahau Location-based Solution

You can deploy your controller and APs as part of an AeroScout or Ekahau location-based solution.

On the controller, you configure the AeroScout/Ekahau server IP address and enable the location-based service. The AeroScout/Ekahau server is aware only of the controller IP address and is notified of the operational APs by the controller.

On the APs that you want to participate in the location-based service, you enable the location-based service.



Note

Participating APs must use the 2.4 GHz band.

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 an AeroScout/Ekahau Wi-Fi RFID tag in the 2.4

GHz band. The tag reports are collected by the AP and forwarded to the AeroScout/Ekaha server by encapsulating the tag reports in a WASSP tunnel and routing them as IP packets through the controller.



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 532.

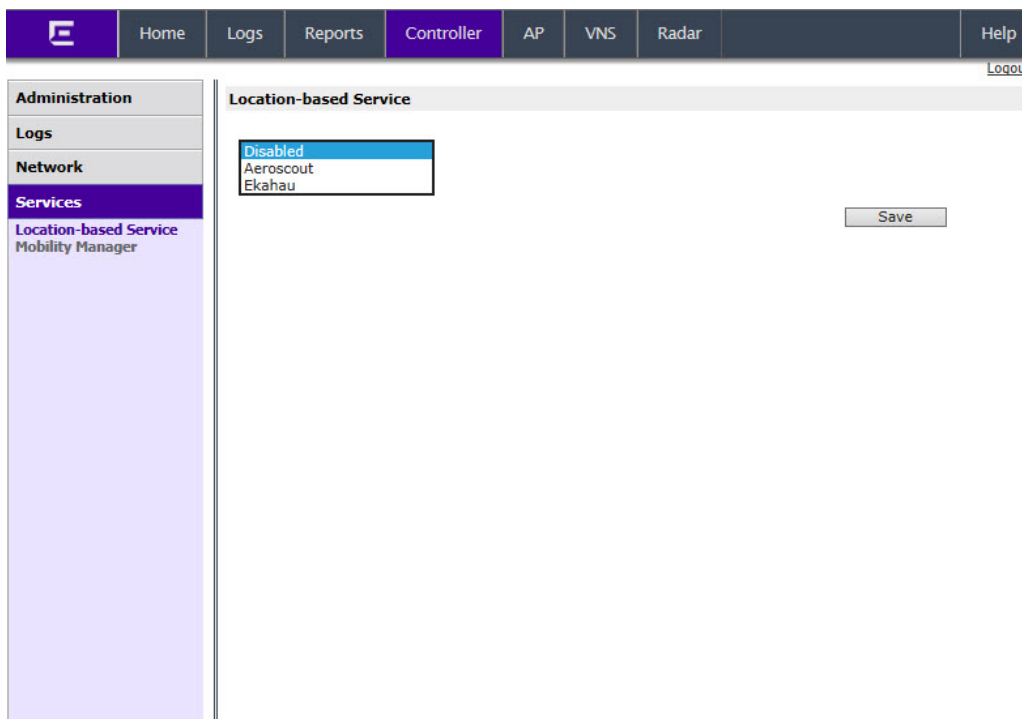
If availability is enabled, tag report transmission pauses on failed over APs until they are configured and notified by the AeroScout/Ekaha server.

When AeroScout/Ekaha support is disabled on the controller, the controller does not communicate with the AeroScout/Ekaha server and the APs do not perform any AeroScout/Ekaha-related functionality.

Ensure that your AeroScout/Ekaha 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. Refer to AeroScout/Ekaha documentation for proper deployment of the AeroScout/Ekaha location-based solution.

To Configure a controller for Use with an AeroScout/Ekaha Solution:

- 1 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Services** > **Location-based Service**. The **Location-based Service** screen displays.



- 3 From the **Location-based Service** drop-down list, click the desired location-based service for the controller.

- If Aeroscout is selected, enter the Server IP Address of the AeroScout server in the **Aeroscout Address** field.

Location-based Service

Aeroscout

Server IP Address:

- If Ekahau is selected, enter the Server IP Address, Server Port, and Multicast Address of the Ekahau server on the **Ekahau Address** field.

Location-based Service

Ekahau

Server IP Address:

Server Port:

Multicast Address:

- Click **Save**.
You must now assign APs to participate in the location-based service.
- From the top menu, click **AP**. In the left pane, click **APs**. The **All APs** screen displays.

AP Properties		
Name	Serial	Model
C4110 - ap1 - AP4102	0002000609223321	Wireless AP4102
C4110 - ap2 - AP3620	0500008043050317	Wireless AP3620 External
C4110 - ap3 - AP3825e	1406000708420000	Wireless AP3825e External

- Select an AP.

- 9 Click **Advanced**. The **Advanced** window displays.



- 10 Select the **Enable location-based service** field.
- 11 Click **Close**. The **Advanced** window closes.
- 12 Repeats steps 7 through 10 for each additional AP that you want to participate in the location-based service.
- 13 Click **Save**.



Note

You can also enable location-based service on APs through the **Location-based service field** on the **AP Multi-edit** screen and the **Advanced** window of the **AP Default Settings** screen.

Additional Ongoing Operations of the System

Ongoing operations of the Extreme Networks Identifi Wireless system can include the following:

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

For more information, see [Performing System Administration](#) on page 544 or the Extreme Networks Identifi Wireless *Maintenance Guide*.

4 Configuring the Identifi Wireless APs

Wireless AP Overview
Discovery and Registration Overview
Wireless AP Default Configuration
Configuring Wireless AP Properties
Configuring Wireless AP Radio Properties
Configuring VLAN Tags for Wireless APs
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 Sensor
Configuring an AP as a Guardian
Performing AP Software Maintenance
Understanding the Identifi Wireless AP LED Status

Wireless AP Overview

Extreme Networks Identifi Wireless APs use the 802.11 wireless standards (802.11a/b/g/n/ac) for network communications, and bridge network traffic to an Ethernet LAN. Wireless APs run proprietary software that allows them to communicate with a controller only.

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 Extreme Networks Identifi Wireless APs supported. AP models are listed in the order of most current models (top) to the oldest models (bottom), with the next-generation 38xx APs being the most recent product series.

The i and e at the end of the product name indicate that the AP has internal (i) or external (e) antennas.

Table 9: Extreme Networks IdentifiFi Wireless APs

AP model	Supported Protocols	Antennas	Features	Radios
38xx Radar Series				
WS-AP3805i WS-AP3805e	802.11a/b/g/n/ac	i – 4 internal e – 4 external	Indoor; Radar capable	2
WS-AP3801i	802.11a/b/g/n/ac	i – 4 internal	Indoor; Radar capable	2
WS-AP3865e	802.11a/b/g/n/ac	e – 6 external	Outdoor; Radar capable	2
WS-AP3825i WS-AP3825e	802.11a/b/g/n/ac	i – 6 internal e – 6 external	Indoor; Radar capable	2
37xx Radar Series				
WS-AP3765i WS-AP3765e	802.11a/b/g/n	i – 6 internal e – 6 external	Outdoor; Radar capable	2
WS-AP3767e	802.11a/b/g/n	e – 6 external	Outdoor; Radar capable; fiber optic instead of copper cable connectors	2
WS-AP3715i WS-AP3715e	802.11a/b/g/n	i – 6 internal e – 6 external	Indoor; Radar capable	2
WS-AP3710i WS-AP3710e	802.11a/b/g/n	i – 6 internal e – 6 external	Indoor; Radar capable	2
WS-AP3705i	802.11a/b/g/n	4 internal	Indoor; Radar capable	2
36xx 11n Series				
WS-AP3660WS- AP3660-1	802.11a/b/g/n	6 external	Outdoor	2
WS-AP3640 WS-AP3630	802.11a/b/g/n	3640: 3 external 3630: 3 internal	Indoor/Outdoor; Standalone	2
WS-AP3620	802.11a/b/g/n	3 external	Indoor	2
WS-AP3610	802.11a/b/g/n	6 internal	Indoor	2
WS-AP3605	802.11a/b/g/n	6 internal	Indoor	2
26xx & 4102 Legacy (pre-11n) Series				
WS-AP2660	802.11a/b/g	4 external	Outdoor	2 dualband
WS-AP2650	802.11a/b/g	2 internal	Outdoor	2 dualband
WS-AP2640 WS-AP2630	802.11a/b/g	2640: 2 external 2630: 2 internal	Indoor; Standalone	2
WS-AP2620	802.11a/b/g	2 external	Indoor	2
WS-AP2610	802.11a/b/g	2 internal	Indoor	2
WS-AP2605	802.11a/b/g	2 internal	Indoor	2
RBT-4102 (RoamAbout series)	802.11a/b/g	2 internal; 2 external	Indoor	2

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 series APs support the 802.11ac wireless protocol.

The AP36xx series APs and the AP3705i deliver 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).

To configure an 802.11n AP to achieve this high link rate, see [Achieving High Throughput with 11n and 11ac Wireless APs](#) on page 152.

Antennas

Some wireless AP models have built-in, internal antennas; some support external antennas. Only the legacy RoamAbout (RBT) models have both. 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 *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 136.

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/Standalone — Most of the APs made by Extreme Networks are controller-based, meaning that they are intended to be controlled centrally by an Identifi Wireless 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.

Standalone APs by default are configurable and connect directly to a wireless LAN without an intermediate controller. They are in effect APs with built-in controllers, connecting to other standalone APs to create a wireless LAN. Standalone APs can be easily converted to perform as standard APs. Currently, AP3630, AP3640 and AP2630, AP2640 are the only standalone APs in the Extreme Networks catalog.

- **Threat Detection and Prevention Capability** —As the potential for wireless security threats grows, APs must also evolve to detect and counter hostile intrusion and attacks. The AP37xx, AP38xx, and W78xC series of access points are designed to support Radar channel monitoring and are configurable for protection against detected attacks. Previous generation wireless APs provide some limited threat detection scanning through the legacy (and still supported) Mitigator feature.

The Radar and Mitigator functions are described in greater detail in [Threat Detection and Prevention Features](#) on page 104. Configuration of these functions on controllers is described in [Working with IdentifiFi Radar](#) on page 456.

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

Radios



Note

The following access point radio discussion does not apply to the AP2650/2660 access points. For more information on the AP2650/2660 access points, see [26xx and Other Legacy Wireless APs](#) on page 199.

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 38xx and AP37xx series radios (except AP3705i) support up to 450Mbps using three spatial streams. 802.11n AP36xx radios support two channel bandwidths, 20 MHz and 40 MHz, at up to 300Mbps in 40 MHz channels and 130Mbps in 20 MHz channels. The modulation used is MIMO-OFDM with one or two spatial streams. When in 802.11a mode, legacy AP radios support data rates up to 54Mbps. The modulation used is OFDM.

The radios are enabled or disabled through the Wireless Assistant. For more information, see [Modifying 11n and 11ac Wireless AP Radio Properties](#) on page 149.

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. To achieve this level of high link rates, specific items need to be configured through the controller. For more information, see [Achieving High Throughput with 11n and 11ac Wireless APs](#) on page 152.

AP4102/4102C Access Points

The AP4102 and AP4102C access points are Extreme Networks first generation access points that run Extreme Networks WLAN software. The AP4102/4102C access point have 2 integrated dual-band antennas. Diversity, which is the use of two antennas to increase the odds that a better radio stream is received on either of the antennas, is supported only with integrated antennas.

Threat Detection and Prevention Features

Identifi Wireless 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 (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 NetSight

AP3705i, AP3710, AP3715, AP3765, AP3767, AP3825, AP3801i, AP3865, W78xC, and AP3805 model 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 37xx, 38xx, and W78xC APs is configured on In-Service Scan Profiles.

AP3710, AP3715, AP376x, AP3825, AP3801i, AP3865, and AP3805 can be configured 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 this 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 and 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.

Existing APs of the earlier Extreme Networks AP36xx and AP26xx product series cannot support full Radar threat scanning and prevention, but they do still continue to support the legacy Mitigator functions as Out-of-Service scan profiles (and must be defined and enabled as such) in the Radar subsystem. Customers upgrading to Radar-compatible convergence software releases will see their legacy scan groups converted to Out-of-Service Scan Profiles. Threat events detected from APs on Out-of-Service Scan Profiles continue to be reported and processed on Wireless Manager (the configuration and management tool for controller and APs), but are not able to trigger alerts or affect the calculated maintenance state of managed devices.

Radar feature configuration is described in [Working with Identifi Radar](#) on page 456.

802.11n-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.

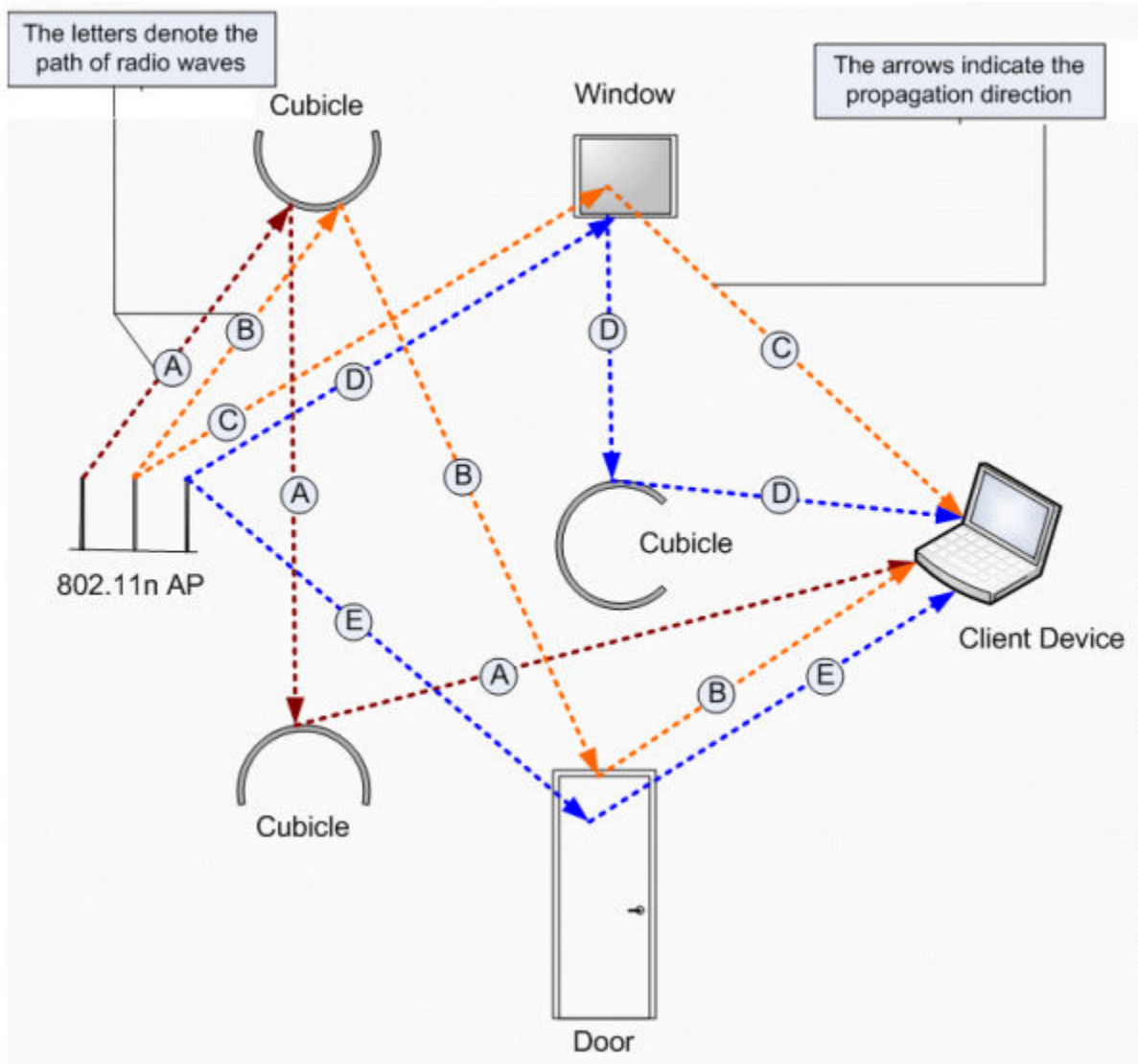
Note



Do not confuse MIMO with the **Diversity** feature. While Diversity is the use of two antennas to increase the odds that a better radio stream is received on either of the antennas, MIMO antennas radiate and receive multi-streams of the same packet to achieve the increased throughput. The **Diversity** feature is meant to offset the liability of RF corruption, arising out of multipath, whereas MIMO converts the liability of multipath to its advantage.

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

Figure 10: MIMO in Wireless APs



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 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 are 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 632.

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 136.

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 Overview](#) on page 112.

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

- **DHCP assignment** — When an AP is powered on, it attempts to reach the DHCP server on the network to acquire an IP address. If the AP is successful in reaching the DHCP server, 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.
 - The AP waits for 30 seconds in default IP address mode before again attempting to acquire an IP address from the DHCP server.
 - The process repeats itself 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 Overview](#) on page 112.

- **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 a telnet or 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 108.

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 143 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 IdentifiFi Wireless Appliance has been installed and connected to the network. For more information, see [Configuring the IdentifiFi Wireless Appliance](#) on page 38.
- The IdentifiFi Wireless Appliance has been configured. For more information, see [Configuring the IdentifiFi Wireless Appliance](#) on page 38.
- The wireless APs have been installed.

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

Once the installations are completed, you can then continue with the AP initial configuration. The AP initial configuration involves two steps:

- 1 Define parameters for the discovery process. For more information, see [Defining Properties for the Discovery Process](#) on page 115.
- 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 subsection describes three methods you can use for modifying the properties of APs in your network.

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

If you have a wireless 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 on the **AP Properties** tab.

To Configure a wireless AP with the System's Default AP Settings:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the **AP** list, click the AP whose properties you want to modify. The **AP Properties** tab displays AP information.

- 3 To have the AP inherit the system's default AP settings, click **Reset to Defaults**. A pop-up dialog asks you to confirm the configuration change.
- 4 To confirm resetting the wireless AP to the default settings, click **OK**.



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

You can modify the system's default AP settings by using the **Copy to Defaults** feature on the **AP Properties** tab. This feature allows the properties of an already configured AP to become the system's default AP settings.

To Modify the System's Default AP Settings Based on an Already Configured AP:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the **AP** list, click the AP whose properties you want to become the system's default AP settings. The **AP Properties** tab is displayed.
- 3 If applicable, modify the AP's properties. For more information, see [AP Properties Tab Configuration](#) on page 138.
- 4 To make this AP's configuration be the system's default AP settings, click **Copy to Defaults**. A pop-up dialog asks you to confirm the configuration change.
- 5 To confirm resetting the system's default AP settings, click **OK**.

Configuring Multiple Wireless APs Simultaneously

In addition to configuring wireless APs individually, you can also configure multiple APs simultaneously by using the AP Multi-edit function. Configuring APs simultaneously is similar to modifying the system's default AP settings or individual APs.

When selecting which APs to configure simultaneously, you can use the following criteria:

- Select the APs by hardware type
- Select the APs individually

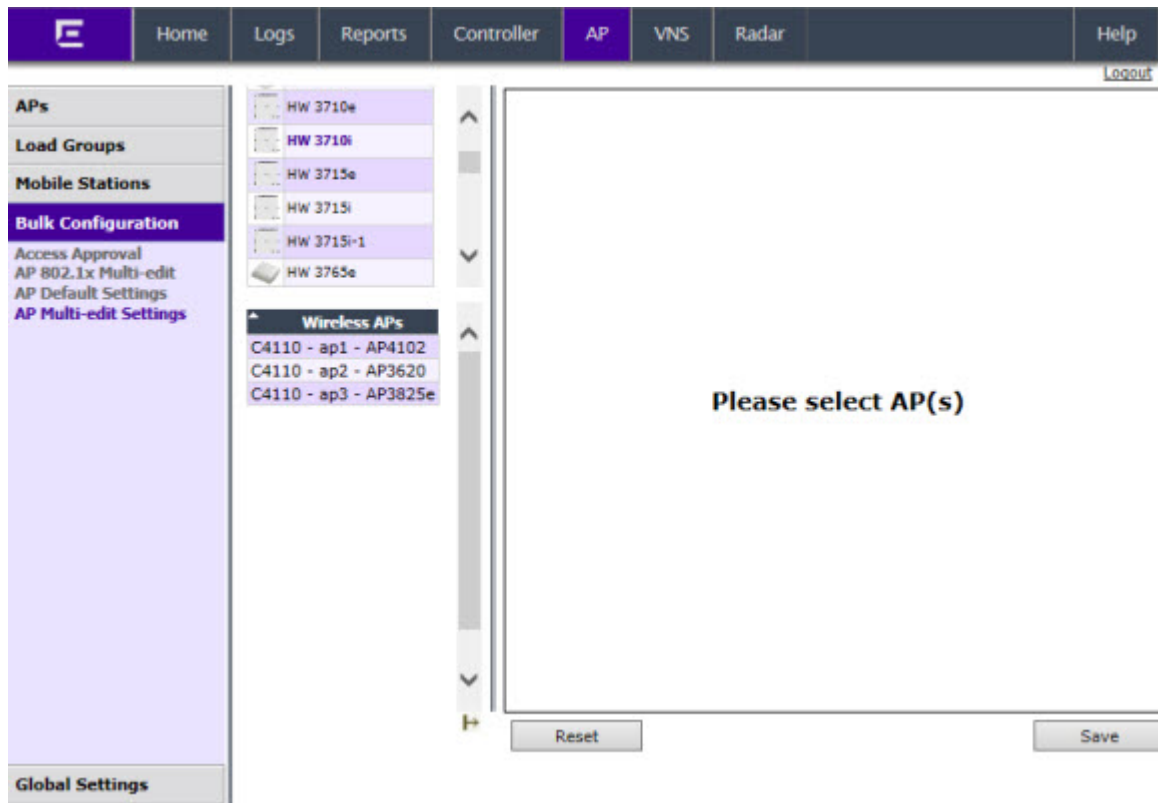
You can select multiple hardware types and individual APs by pressing the Ctrl key and selecting the hardware types and specific APs.

When you configure multiple APs using the AP Multi-edit screen, it is important to note that for some AP settings to be available for configuration, other AP settings must be enabled or configured first. Only settings and options supported by all of the currently selected hardware types are available for configuring.

To Configure Wireless APs Simultaneously:

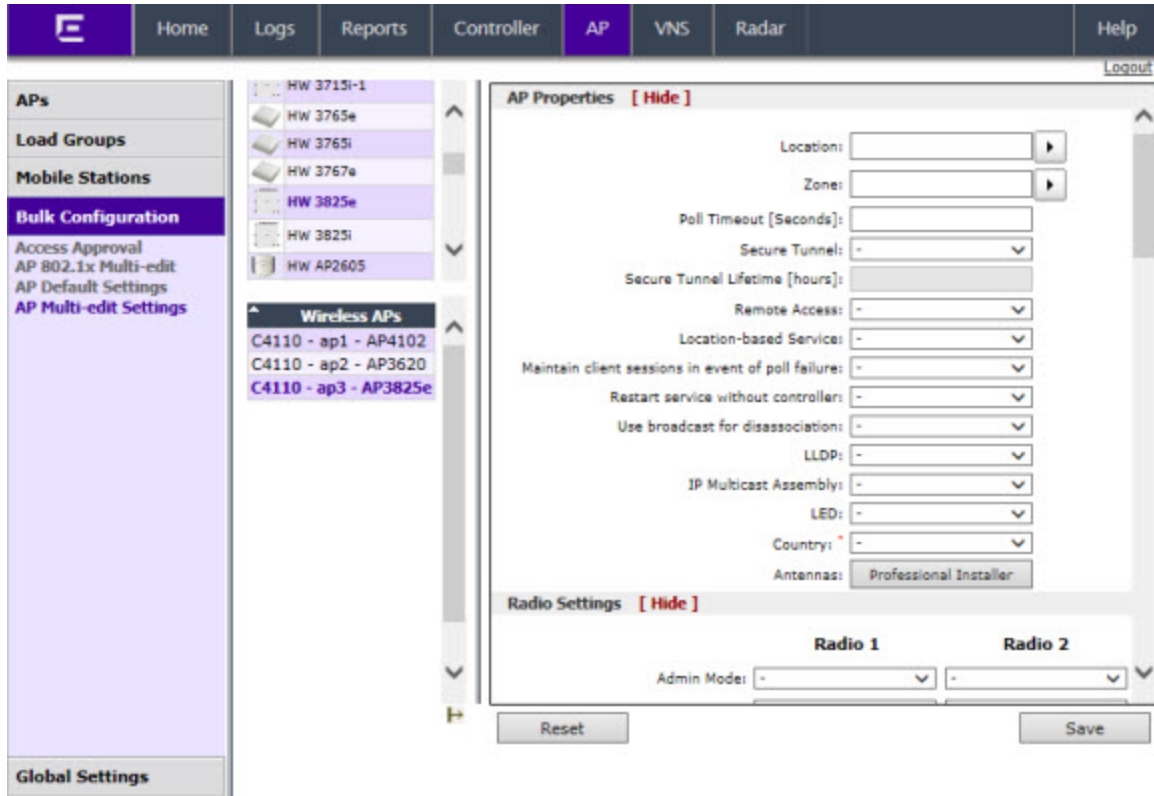
- 1 From the top menu, click **AP**. The **AP** screen displays.

- 2 In the left pane, click **Bulk Configuration** > AP Multi-edit Settings.



- 3 In the **Wireless APs** list, select one or more APs to edit. To select multiple APs, click the APs on the list and press the CTRL key with each click. The AP profile page displays.

You can use the **Hardware Types** list to narrow down the APs by type. When you select one or more hardware types from that list, APs of that type are highlighted in the APs list. In the following AP profile page example, the AP2620 hardware type is selected and the only AP2620 in the Wireless APs list is highlighted.



When you use the **Multi-edit** function, any box or option that is not explicitly modified is not changed by the update. The APs shown in the **Wireless APs** list can be from any version of the software. Only attributes that are common between software versions are available for multi-edit. Setting an attribute that does not apply to an AP does not cause an abort of the multi-edit operation.

Table 10: AP Multi-edit Properties

Field/Button	Description
Hardware Types	The AP hardware model.
Wireless APs	The name assigned to the AP.
AP Properties	For more information, see AP Properties Tab Configuration on page 138.
Radio Settings	For more information, see Configuring Wireless AP Radio Properties on page 147.
Static Configuration	
EWC Search List	Click one of the following: <ul style="list-style-type: none"> Clear search list — Click to clear previously assigned controllers that were configured to control this AP. Re-configure search list — Click to assign controllers to control this AP. This causes the Add box to become available.

Table 10: AP Multi-edit Properties (continued)

Field/Button	Description
Add box	<p>Enter the IP address of the controller that controls this AP. This box is available only if you selected Re-configure search list when configuring the search list.</p> <p>Click the Add button to add the IP address to the list. Repeat to add additional controllers. The maximum is three controllers.</p> <p>Click Up and Down to modify the order of the controllers.</p> <p>The AP is successful when it finds an controller that allows it to register.</p> <p>This feature allows the AP to bypass the discovery process. If the EWC Search List 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 Overview on page 112.</p>
Tunnel MTU	<p>Enter a static MTU value, from 600 to 1500. 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 56). If the Extreme Networks 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.</p>
WLAN Assignments	
WLAN Assignments	<p>From the drop-down list, click one of the following:</p> <ul style="list-style-type: none"> • Clear WLAN list — Click to clear previously assigned WLAN services of the APs. • Re-configure WLAN list — Click to assign WLAN services to the APs. <p>In the Radio 1 and Radio 2 columns, select the AP radios that you want to assign for each WLAN service.</p>
Save	Click to save your changes.

Discovery and Registration Overview

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 (see [Figure 11: Wireless AP Discovery Process](#) on page 113). When the discovery process is successful, the AP registers with the controller.



Warning

Only use power supplies that are recommended by Extreme Networks. For example, an AP3610 uses WS-PS361020-MR (AP3610/AP3620 AC Power Supply-Multi-Region).

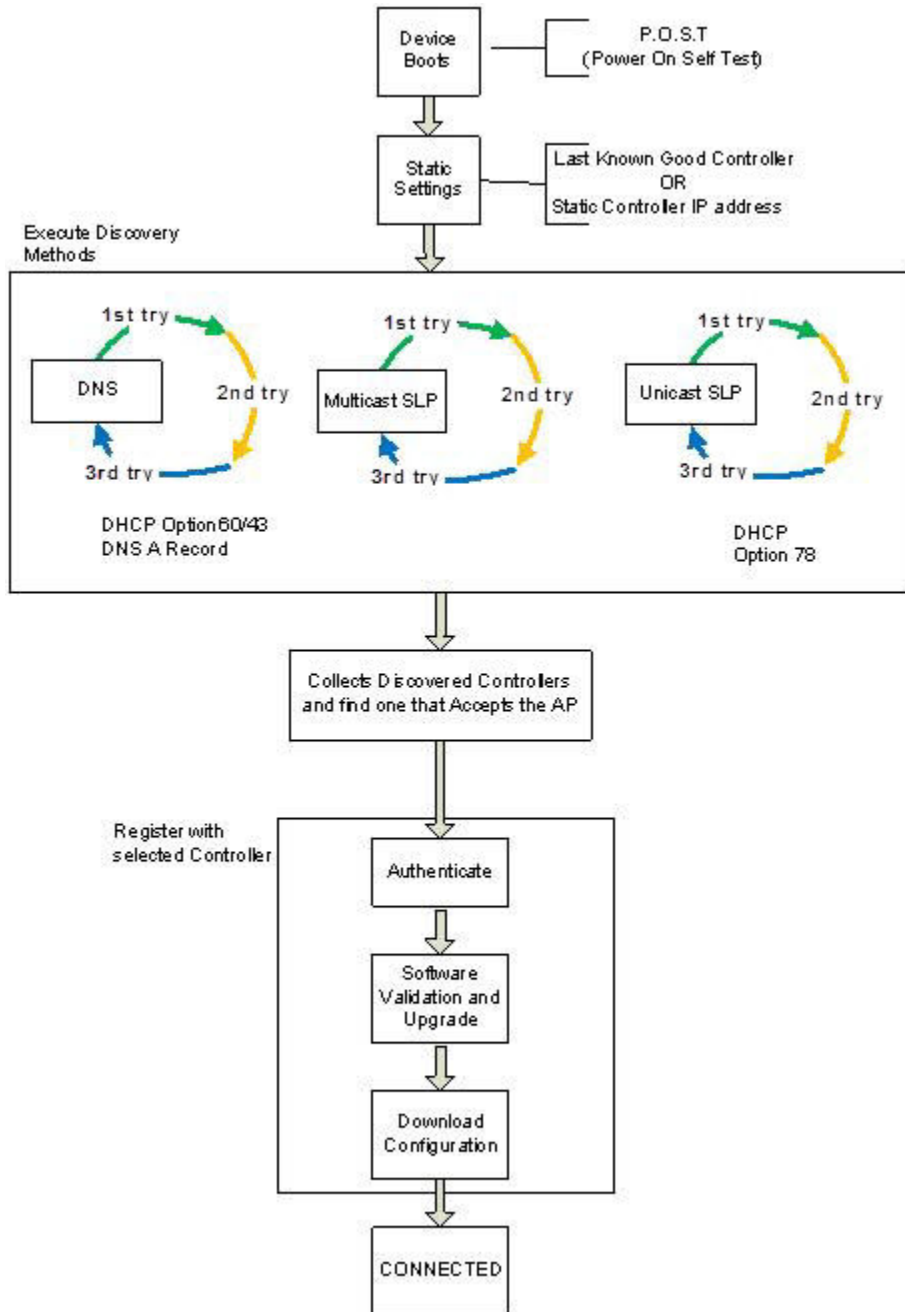


Figure 11: Wireless AP Discovery Process

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 Dynamic Host Configuration Protocol (DHCP) Option 60 to query the DHCP server for available controllers. The DHCP server responds to the AP with Option 43, which lists the available controllers.

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

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

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

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

- 5 Use a multicast SLP request to find SLP SAs

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

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

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

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

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

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

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

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

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

Defining Properties for the Discovery Process

Before a wireless AP is configured, define the following properties for the discovery process:

- [Security Mode](#) on page 115
- [Discovery Timers](#) on page 116

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 136.

Discovery Timers

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

To Define the Discovery Process Parameters:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Global Settings** > AP Registration. The **Wireless AP Registration** screen displays.

The screenshot shows the 'Wireless AP Registration' configuration page. The left sidebar contains a navigation menu with 'Global Settings' selected, and sub-items for 'AP Maintenance', 'AP Registration', and 'WAS Sensor Management'. The main content area is titled 'Wireless AP Registration' and includes the following sections:

- Security Mode:** Two radio buttons. The first, 'Allow all Wireless APs to connect', is selected. The second is 'Allow only approved Wireless APs to connect'.
- Discovery Timers:** Two input fields. 'Number of retries' is set to 3 (range 1-255). 'Delay between retries' is set to 3 (range 1-10 seconds).
- Telnet Access:** Two password input fields with 'Unmask' buttons.
- SSH Access:** Two password input fields with 'Unmask' buttons.
- Secure Cluster:** A 'Cluster Shared Secret' field with masked characters and an 'Unmask' button. Two checkboxes are checked: 'Use Cluster Encryption' and 'Inter AP Roam'.

At the bottom of the page, there are two buttons: 'View SLP Registration' and 'Save'.

- 3 In the **Security Mode** section, select one of the following:
 - **Allow all Wireless APs to connect** option is selected by default. For more information, see [Security Mode](#) on page 115.
 - **Allow only approved Wireless APs to connect**
- 4 In the **Discovery Timers** section, type the discovery timer values in the following boxes:
 - **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.

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

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.

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 All APs screen displays.

AP Properties		
Name	Serial	Model
C4110 - ap1 - AP4102	0002000609223321	Wireless AP4102
C4110 - ap2 - AP3620	0500008043050317	Wireless AP3620 External
C4110 - ap3 - AP3825e	1406000708420000	Wireless AP3825e External

- 2 To view detailed information on a specific AP, click the AP from the list in the right-pane. For more information, see [AP Properties Tab Configuration](#) on page 138.
- 3 To add a new AP to the list, click **New**. For more information, see [Manually Adding and Registering a Wireless AP](#) on page 118.

Manually 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 136).

To add and register an AP manually:

- 1 From the top menu, click **AP**. The **AP** screen displays.

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

- 2 Click **New**.

The **Add Wireless AP** screen displays.

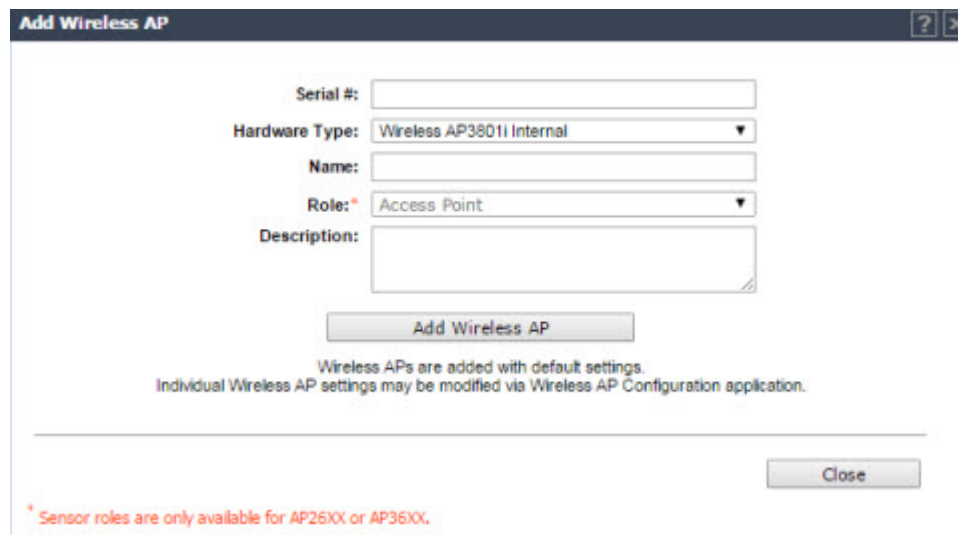


Table 11: Add Wireless AP window

Field	Description
Serial #	Type the unique identifier of the AP.
Hardware Type	Select the hardware model of this AP from the drop-down menu
Name	Type a unique name for the AP that identifies the access point. The default value is the AP's serial number.
Role	Select the role for this AP: access point or sensor. If the hardware type you select supports only the access point role, the items in the drop-down list may be view-only. Only certain AP hardware types support the sensor role.
Description	Enter a description of this AP.

Table 11: Add Wireless AP window (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.

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.

The process of configuring the default AP settings is divided into up to six tabs:

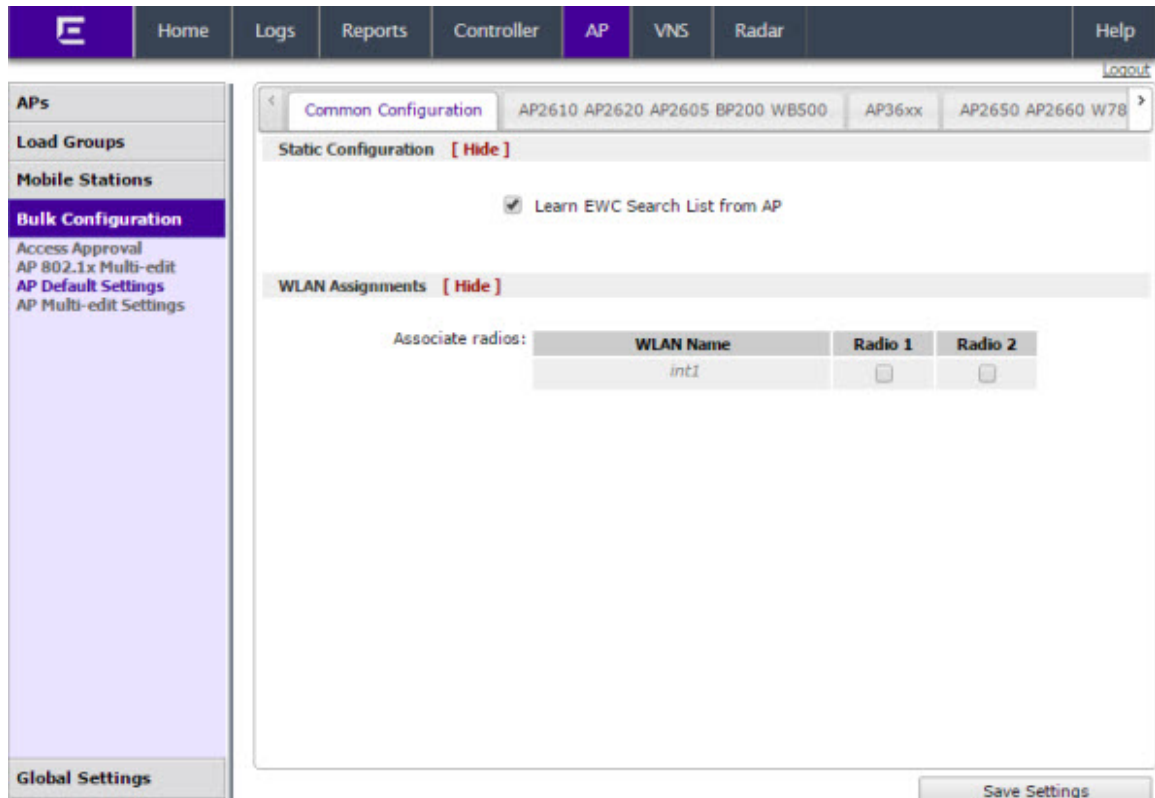
- **Common Configuration** — Configure common configuration, such as WLAN assignments and static configuration options for all APs. See [Configuring Common Configuration Default AP Settings](#) on page 119.
- **AP2610 AP2620 AP2605 BP200 WB500** — Configure the default settings for the legacy APs, and the BP200, and WB500 access points. See [Configuring Default AP Settings](#) on page 126.
- **AP36xx** — Configure the default settings for the 11n APs. See [Configuring AP36xx Default AP Settings](#) on page 123.
- **AP2650 AP2660 W786** — Configure the default settings for the legacy outdoor APs. See [Configuring AP2650/AP2660, W786 Default AP Settings](#) on page 124.
- **AP4102x** — Configure the default settings for the AP4102 and the AP4102C access points. See [Configuring AP4102x Default AP Settings](#) on page 125.
- **AP37xx W78xC**— Configure the default settings for the Radar series APs. See [Configuring AP37xx, W78xC Default AP Settings](#) on page 121.
- **AP38xx**— Configure the default settings for the Identifi Radar series APs. See [Configuring AP38xx Default AP Settings](#) on page 121.
- **AP3801**— Configure the default settings for the Identifi Radar series APs. See [Configuring AP3801 Default AP Settings](#) on page 122.

Configuring Common Configuration Default AP Settings

To Configure Common Configuration Default AP Settings:

- 1 From the top menu, click **AP**. The **AP** screen displays.

- In the left pane, click **Bulk Configuration**, then **AP Default Settings**. The **Common Configuration** tab is displayed.



- In the **Static Configuration** section, do one of the following:
 - To allow each AP to provide its own EWC Search List, select the Learn EWC Search List form AP checkbox.
 - To specify a common EWC Search List for all APs, clear the Learn EWC Search List form AP checkbox.

The AP is successful when it finds a controller that allows it to register.

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.

The DHCP function for wireless clients must be provided locally by a local DHCP server, unless each wireless client has a static IP address.

For the initial AP deployment, it is necessary to use one of the described options in [Discovery and Registration Overview](#) on page 112.

- In the **WLAN Assignments** section:
 - 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 430.
 - To assign Associate radios for each VNS in the list, select the box next to each radio.
- To save your changes, click **Save Settings**.

Configuring AP37xx, W78xC Default AP Settings

To Configure AP37xx, W78xC Default AP Settings:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Bulk Configuration**, then **AP Default Settings**. The **Common Configuration** tab is displayed.
- 3 Click the **AP37xx W78xC** tab.

The screenshot shows the configuration interface for AP37xx W78xC. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar shows the navigation menu with 'Bulk Configuration' selected. The main content area is divided into 'AP Properties' and 'Radio Settings' sections.

AP Properties [Hide]

- LLDP: Disabled
- Country: United States

Radio Settings [Hide]

	Radio 1	Radio 2
Admin Mode:	On	On
Radio Mode:	a/n	g/n
Channel Width:	40MHz	20MHz
RF Domain:	MyDomain	MyDomain
Auto Tx Power Ctrl:	Off	Off
Max Tx Power:	18 dBm	18 dBm
Min Tx Power: ¹	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust:	0 dB	0 dB
Channel Plan:	All Non-DFS-Channe	Auto
Antenna Selection: ⁴	Left/Middle/Right	Left/Middle/Right

¹ Minimum power level is subject to the regulatory compliance requirement for the selected country
⁴ This setting may require APs to reboot

Buttons: Advanced..., Save 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 127.

- 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**. The **AP** screen displays.
- 2 In the left pane, click **Bulk Configuration**, then **AP Default Settings**. The **Common Configuration** tab is displayed.

- Click the **AP38xx** tab.

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

For detailed information, see [AP Default Settings](#) on page 127.

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

Configuring AP3801 Default AP Settings

To Configure AP3801 Default AP Settings:

- From the top menu, click **AP**. The **AP** screen displays.
- In the left pane, click **Bulk Configuration**, then **AP Default Settings**. The **Common Configuration** tab is displayed.

- Click the **AP3801** tab.

The screenshot shows the configuration page for AP3801. The top navigation bar includes Home, Logs, Reports, Controller, AP (selected), VNS, Radar, and Help. The left sidebar has APs, Load Groups, Mobile Stations, Bulk Configuration (selected), Access Approval, AP 802.1x Multi-edit, AP Default Settings, and AP Multi-edit Settings. The main content area shows AP Properties (LLDP: Disabled, Country: United States) and Radio Settings for Radio 1 and Radio 2. The Radio 1 settings are: Admin Mode: On, Radio Mode: a/n/ac, Channel Width: 80MHz, RF Domain: MyDomain, Auto Tx Power Ctrl: Off, Max Tx Power: 18 dBm, Min Tx Power: 0 dBm, Auto Tx Power Ctrl Adjust: 0 dB, and Channel Plan: All Non-DFS-Channe. The Radio 2 settings are: Admin Mode: Off, Radio Mode: b/g/n, Channel Width: Auto, RF Domain: MyDomain, Auto Tx Power Ctrl: Off, Max Tx Power: 18 dBm, Min Tx Power: 8 dBm, Auto Tx Power Ctrl Adjust: 0 dB, and Channel Plan: Auto. There are two red footnotes: '1 Minimum power level is subject to the regulatory compliance requirement for the selected country' and '* This setting may cause APs to reboot.' Buttons for 'Advanced...', 'Save Settings', and 'Logout' are visible.

- Configure the following Default AP Settings as required:

- AP Properties
- Radio Settings
- Advanced Settings

For detailed information, see [AP Default Settings](#) on page 127.

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

Configuring AP36xx Default AP Settings

To Configure AP36xx Default AP Settings:

- From the top menu, click **AP**. The **AP** screen displays.
- In the left pane, click **AP Default Settings**. The **Common Configuration** tab is displayed.

- 3 Click the **AP36xx** tab.

The screenshot shows the configuration interface for an AP36xx. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar has 'APs', 'Load Groups', 'Mobile Stations', and 'Bulk Configuration' (selected). The main content area has tabs for 'Common Configuration', 'AP2610 AP2620 AP2605 BP200 WB500', 'AP36xx', and 'AP2650 AP2660 W78'. The 'AP Properties' section shows 'LLDP: Disabled' and 'Country: United States'. The 'Radio Settings' section is expanded to show configurations for Radio 1 and Radio 2. The configurations are as follows:

Setting	Radio 1	Radio 2
Admin Mode	Off	On
Radio Mode	a/n	b/g
Channel Width	40MHz	20MHz
RF Domain	MyDomain	MyDomain
Auto Tx Power Ctrl	Off	Off
Max Tx Power	18 dBm	18 dBm
Min Tx Power	0 dBm	8 dBm
Auto Tx Power Ctrl Adjust	0 dB	0 dB
Channel Plan	All Non-DFS-Channel	Auto
Antenna Selection	Left/Middle/Right	Left/Middle/Right

Footnotes:
¹ Minimum power level is subject to the regulatory compliance requirement for the selected country
² This setting may require AP to reboot

Buttons: 'Advanced...', 'Save 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 127.

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

Configuring AP2650/AP2660, W786 Default AP Settings

To Configure AP2650/AP2660, W786 Default Access Point Settings:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **AP Default Settings**. The **Common Configuration** tab is displayed.
- 3 Click the **AP2650 AP2660 W786** tab.

The screenshot shows the configuration interface for wireless APs. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar has sections for APs, Load Groups, Mobile Stations, Bulk Configuration (with sub-items: Access Approval, AP 802.1x Multi-edit, AP Default Settings, AP Multi-edit Settings), and Global Settings. The main content area is titled 'Common Configuration' and shows settings for AP2650, AP2660, and W786. Under 'AP Properties', LLDP is set to 'Disabled' and Country is 'United States'. The 'Radio Settings' section is expanded to show configurations for Radio 1 and Radio 2:

	Radio 1	Radio 2
Admin Mode:	Off	On
Radio Mode:	a	b/g
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-Channe	Auto

Below the settings, there are two red warning messages:

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

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

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

For detailed information, see [AP Default Settings](#) on page 127.

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

Configuring AP4102x Default AP Settings

To Configure AP4102x Default AP Settings:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **AP Default Settings**. The **Common Configuration** tab is displayed.
- 3 Click the **AP4102x** tab.

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

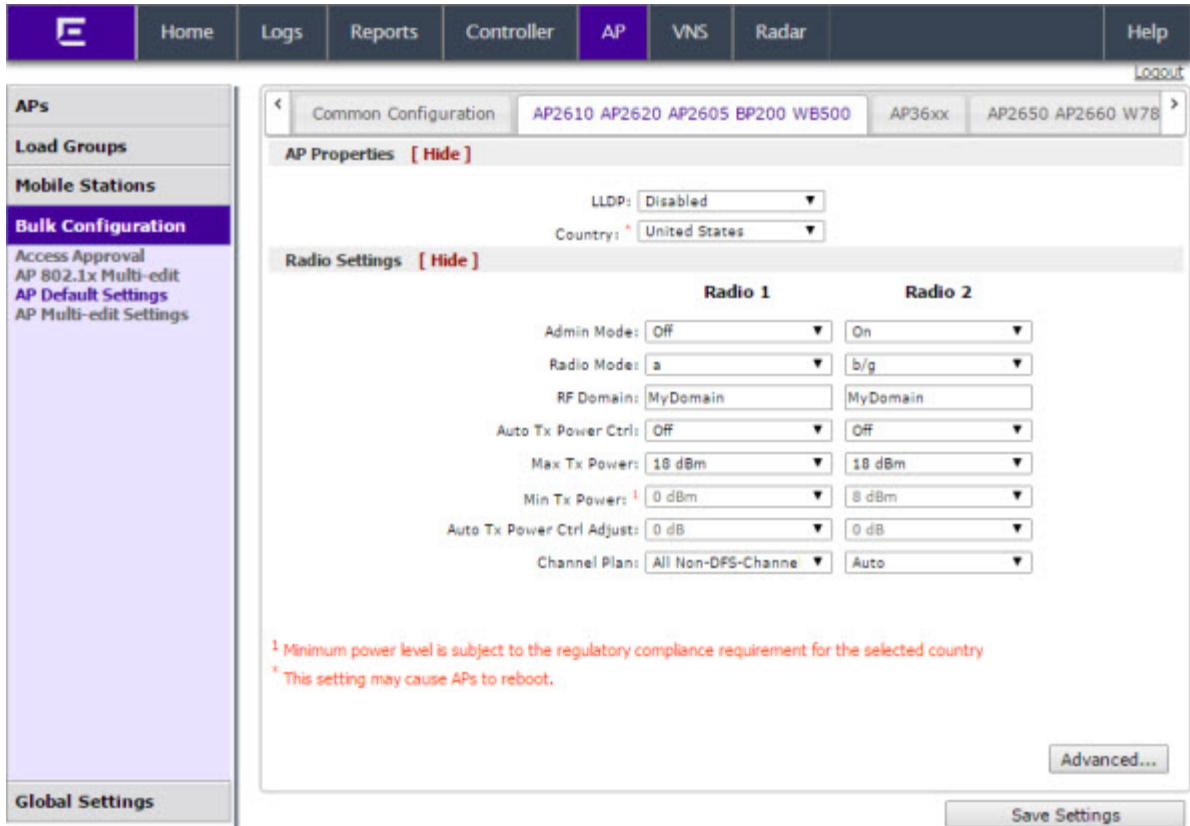
For detailed information, see [AP Default Settings](#) on page 127.

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

Configuring Default AP Settings

To Configure AP2610/20, AP2605, BP200, and WB500 Default AP Settings:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **AP Default Settings**. The **Common Configuration** tab is displayed.
- 3 Click the **AP2610 AP2620 AP2605 BP200 WB500** tab.



4 Configure the following Default AP Settings as required:

- AP Properties
- Radio Settings
- Advanced Settings

For detailed information, see [AP Default Settings](#) on page 127.

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

AP Default Settings

Table 12: AP Default Settings

Field	Description
AP Properties	
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 using SNMP, see the Extreme Networks IdentifiFi Wireless <i>Maintenance Guide</i>

Table 12: AP Default Settings (continued)

Field	Description
Announcement Interval	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.
Announcement Delay	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. Note: The Time to Live value cannot be directly edited. The Time to Live value is calculated as four times the Announcement Interval value.
Country	Click the country of operation. This option is available only with certain licenses.
Radio Settings (Radio 1 and Radio 2)	
Admin mode	Select On to enable this radio; Select Off to disable this radio.
Radio mode	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 147. Depending on the radio modes you select, some of the radio settings may not be available for configuration.
Channel Width	Click the channel width for the radio: <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 Radio 1 only. Auto — Click to automatically switch between 20 MHz, 40 MHz, and 80 MHz channel widths, depending on how busy the extension channel is.
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.

Table 12: AP Default Settings (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>
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. 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. Extreme Networks recommends that use 0 dBm 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>

Table 12: AP Default Settings (continued)

Field	Description
Channel Plan	<p>If ACS is enabled you can define a channel plan for the AP. Defining a channel plan allows you to 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.
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 IdentifiFi Wireless Assistant. Also, the radio is reset causing client connections on this radio to be lost.</p> <p>Note: Antenna Selection is not applicable to the AP26XX, 4102, or Outdoor AP3660 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 438.</p>

Table 12: AP Default Settings (continued)

Field	Description
Secure Tunnel	<p>This feature, when enabled, provides encryption, authentication, and key management between the AP and/or controllers.</p> <p>Select the desired Secure Tunnel mode from the drop-down list:</p> <ul style="list-style-type: none"> • Disabled — Secure Tunnel is turned off and no traffic is encrypted. All SFTP/SSH/TFTP traffic works normally. • Encrypt control traffic between AP & Controller — An IPSEC tunnel is established from the AP to the controller and all SFTP/SSH/TFTP/WASSP control traffic is encrypted. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. • Encrypt control and data traffic between AP & Controller — This mode only benefits routed/bridged@AP 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. • 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>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>
Remote Access	Click to Enable or Disable telnet access or 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 remaining active if a link loss with the controller occurs. This option is enabled 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.

Table 12: AP Default Settings (continued)

Field	Description
Use broadcast for disassociation	<p>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:</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>
IP Multicast Assembly	Click to Enable or Disable multicast frames assembling for groups of APs using AP Multi-editing settings (for more information, see Configuring Multiple Wireless APs Simultaneously on page 109).
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	Type the desired 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 unfragmented.
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.

Table 12: AP Default Settings (continued)

Field	Description
Dynamic Channel Selection	<p>Click one of the following:</p> <ul style="list-style-type: none"> • Off — Disables DCS. • 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 — If DCS is enabled, type the noise interference level, measured in dBm, above which ACS scans for a new operating channel for the AP if the threshold is exceeded. • DCS Channel Occupancy Threshold — If DCS is enabled, type the channel utilization level, measured as a percentage, above which ACS scans for a new operating channel for the AP if the threshold is exceeded. • DCS Update Period — If DCS is enabled, 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 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)	<p>Enable or disable the following DCS Events:</p> <ul style="list-style-type: none"> • Bluetooth • Microwave • Cordless Phone • Constant Wave • Video Bridge
Rx Diversity	Click Best for the best signal from both antennas, or Left or Right to choose either of the two diversity receiving antennas. The default and recommended selection is Best. If only one antenna is connected, use the corresponding Left or Right diversity setting. Do not use Best if two identical antennas are not used.

Table 12: AP Default Settings (continued)

Field	Description
Tx Diversity	Click Alternate for the best signal from both antennas, or Left or Right to choose either of the two diversity receiving antennas. The default selection is Alternate that maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to Alternate. Under those circumstances, Extreme Networks recommends that you use either Left or Right for Tx Diversity. If only one antenna is connected, use the corresponding Left or Right diversity setting. Do not use Alternate if two identical antennas are not used.
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.
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	<p>For each radio, click the minimum data rate that must be supported by all stations in a BSS:</p> <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. <p>If necessary, the Max Basic Rate choices adjust automatically to be higher or equal to the Min Basic Rate. If both Min Basic Rate and Max Basic Rate are set to an 11g-specific (OFDM) rate, (for example, 6, 12, or 24 Mbps) all basic rates are 11g-specific.</p>

Table 12: AP Default Settings (continued)

Field	Description
Max. Basic Rate	<p>For each radio, click the maximum data rate that must be supported by all stations in a BSS:</p> <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. <p>If necessary, the Max Basic Rate choices adjust automatically to be higher or equal to the Min Basic Rate. If both Min Basic Rate and Max Basic Rate are set to an 11g-specific (OFDM) rate, (for example, 6, 12, or 24 Mbps) all basic rates are 11g-specific.</p>
Max. Operational Rate	<p>For each radio, click the maximum data rate that clients can operate at while associated with the AP:</p> <ul style="list-style-type: none"> Click: 1, 2, 5.5, or 11 Mbps for 11b-only mode. Click 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps for 11b + 11g modes. Click 6, 9, 12, 18, 24, 36, 48, or 54 Mbps for 11g mode. Click 6, 9, 12, 18, 24, 36, 48, or 54 Mbps for 11a mode. <p>If necessary, the Max Operational Rate choices adjust automatically to be higher or equal to the Min Basic Rate.</p>
Adaptive Rate Control	
Background BK	For each radio, click the number of retries for the Background transmission queue. The default value is adaptive (multi-rate). The recommended setting is adaptive (multi-rate).
Best Effort BE	For each radio, click the number of retries for the Best Effort transmission queue. The default value is adaptive (multi-rate). The recommended setting is adaptive (multi-rate).
Video VI	For each radio, click the number of retries for the Video transmission queue. The default value is adaptive (multi-rate). The recommended setting is adaptive (multi-rate).
Voice VO	For each radio, click the number of retries for the Voice transmission queue. The default value is adaptive (multi-rate). The recommended setting is adaptive (multi-rate).
Turbo Voice TVO	For each radio, click the number of retries for the Turbo Voice transmission queue. The default value is adaptive (multi-rate). The recommended setting is adaptive (multi-rate).
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.
40 MHz Prot. Channel Offset	Select a 20 MHz channel offset if the deployment is using channels that are 20 MHz apart (for example, using channels 1, 5, 9, and 13) or a 25 MHz channel offset if the deployment is using channels that are 25 MHz apart (for example, using channels 1, 6, and 11).

Table 12: AP Default Settings (continued)

Field	Description
40 MHz 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 (Available for 37xx, 38xx, and W78xC APs.)	Click an LDPC mode: Enabled or Disabled. LDPC increases the reliability of the transmission resulting in a 2dB increased performance compared to traditional 11n coding.
STBC (Available for 37xx, 38xx, and W78xC APs.)	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 (Available for 37xx, 38xx, and W78xC APs.)	Click a TxBF mode: Enabled or Disabled. 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.

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 137
- [AP Properties Tab Configuration](#) on page 138
- [Setting Up the Wireless AP Using Static Configuration](#) on page 143
- [Configuring Telnet/SSH Access](#) on page 146

When configuring APs, you can choose to configure individual APs or simultaneously configure a group of APs. For more information, see [Configuring Multiple Wireless APs Simultaneously](#) on page 109.

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.

For more information, see [Security Mode](#) on page 115.

AP Rehoming

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.

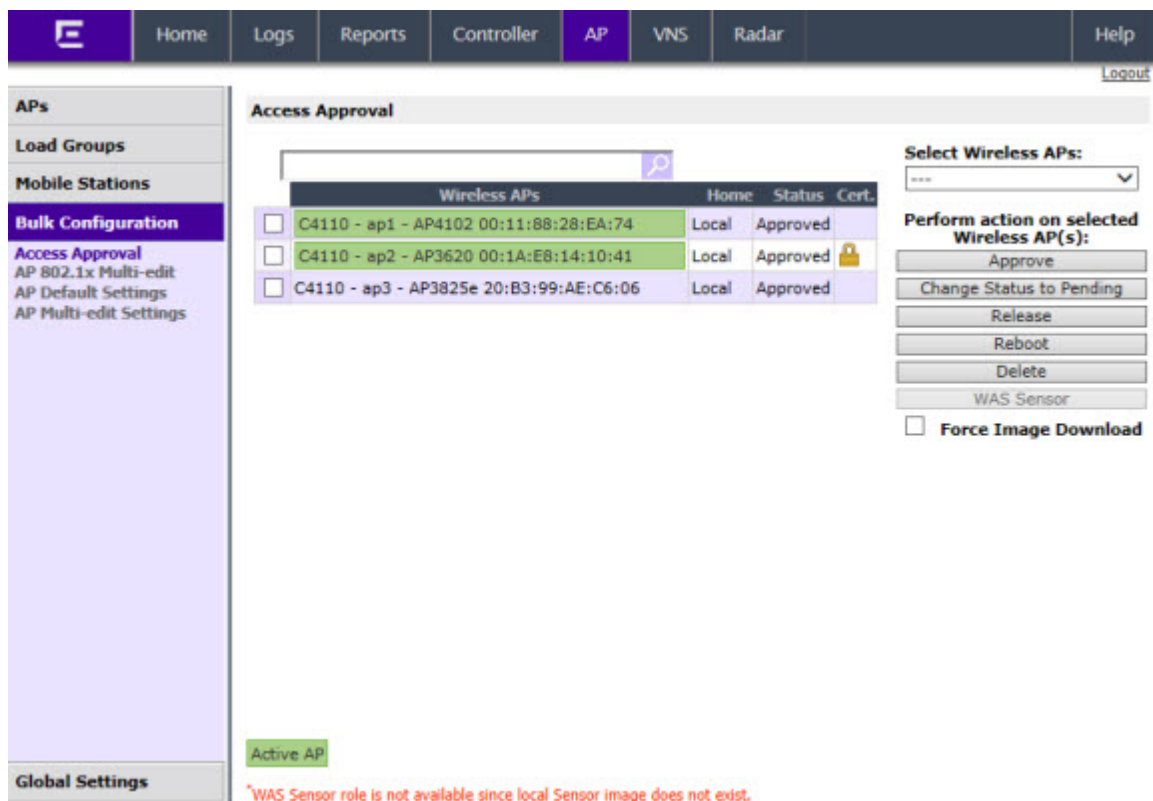
- WLAN assignments are not affected by rehoming.
- WDS and Mesh APs cannot be converted from local to foreign.
- A rehomed AP will be removed from load balance groups.

Modifying an AP's Registration Status

To modify an AP's registration status:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Bulk Configuration**, then **Access Approval**.

The **Access Approval** screen displays, along with the registered APs and their status.



The screenshot displays the 'Access Approval' interface. At the top, a navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. A left sidebar lists 'APs', 'Load Groups', 'Mobile Stations', 'Bulk Configuration', 'Access Approval', 'AP 802.1x Multi-edit', 'AP Default Settings', 'AP Multi-edit Settings', and 'Global Settings'. The main content area shows a table of 'Wireless APs' with columns for 'Home', 'Status', and 'Cert.'. The table lists three APs: 'C4110 - ap1 - AP4102 00:11:88:28:EA:74', 'C4110 - ap2 - AP3620 00:1A:E8:14:10:41', and 'C4110 - ap3 - AP3825e 20:B3:99:AE:C6:06'. All have a 'Local' home and 'Approved' status. The second AP has a lock icon in the 'Cert.' column. To the right, a 'Perform action on selected Wireless AP(s):' section contains buttons for 'Approve', 'Change Status to Pending', 'Release', 'Reboot', 'Delete', and 'WAS Sensor', along with a 'Force Image Download' checkbox. A red error message at the bottom reads: '*WAS Sensor role is not available since local Sensor image does not exist.'

- 3 To select the APs for status change, do one of the following:
 - Search for a specific AP by entering the AP in the search bar and clicking (🔍).
 - For a specific AP, select the corresponding checkbox.
 - For APs by category, click one of the **Select Wireless APs** options.

To clear your AP selections, click **Deselect All**.

- 4 Click the appropriate **Perform action on selected Wireless APs** option:
 - **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 rehomming 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 rehomming is enabled.
 - **Change Status to Pending** — AP is removed from the Active list, and is forced into discovery.
 - **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 430.
 - **Reboot** — Reboot the AP without using Telnet or SSH to access it.
 - **Delete** — Releases the AP from the controller and deletes the AP's entry in the controller's management database.

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**. The **AP** screen displays.
- 2 Click the **APs** button in the left pane, then in the AP list, click the AP whose properties you want to modify. The **AP Properties** tab displays AP information.

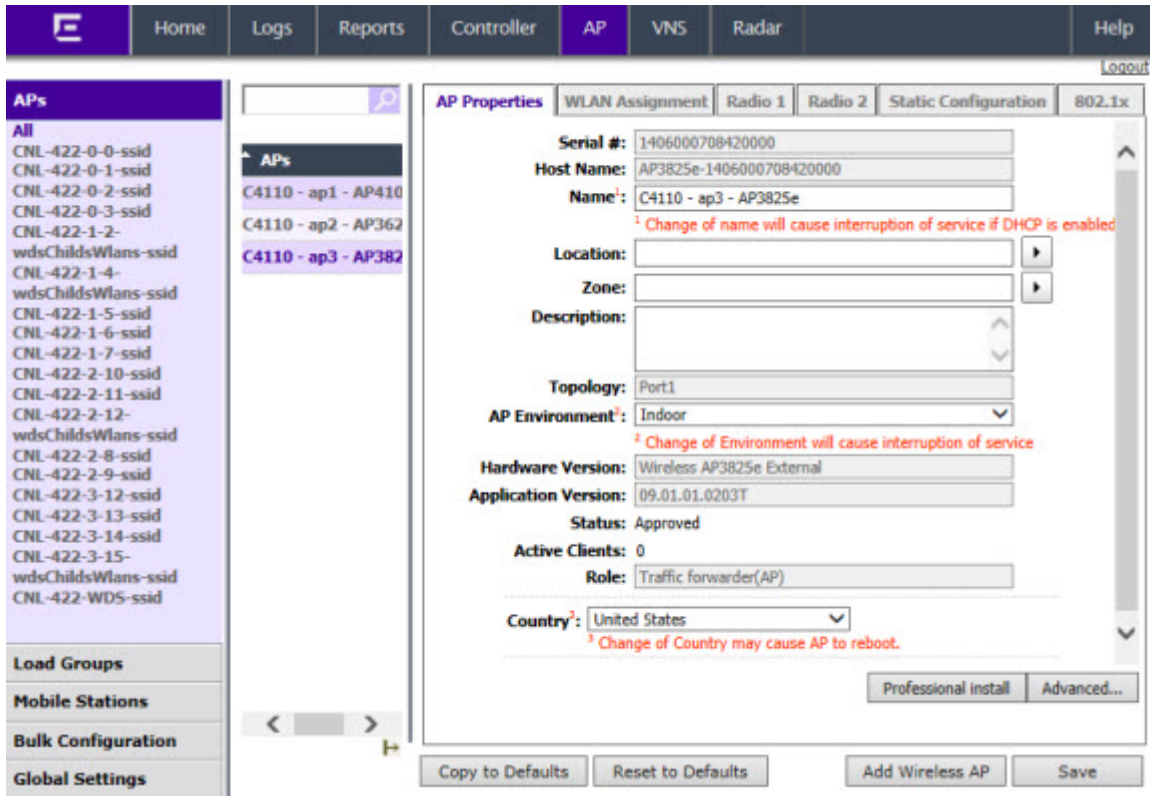


Table 13: AP Properties Tab

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 DHCP 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 486) or the AP Location field. When the clients change areas, a notification is sent.
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.

Table 13: AP Properties Tab (continued)

Field	Description
AP Environment	Click the AP's environment — Indoor or Outdoor. Note: The AP Environment drop-down is displayed on the AP Properties tab only if the selected AP is an Outdoor AP. The Outdoor APs can be deployed in both indoor and outdoor environments.
Hardware Version	Read-only. Displays the current version of the AP hardware.
Application Version	Read-only. Displays the current version of the AP software.
Status	Approved — Indicates that the AP has received its binding key from the controller after the discovery process. If no status is shown, that indicates that the AP has not yet successfully been approved for access with the secure controller. 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 137.
Active Clients	Displays the number of wireless devices currently associated with the AP.
Role	Click the role for the AP. Options include: <ul style="list-style-type: none"> • Traffic Forwarding — Normal Operation. Applies to all APs. • Sensor — Once the AP is configured as a Sensor, the AP no longer performs RF services and is no longer managed by the IdentifiFi Wireless Appliance. Applies to AP26xx/AP36xx only. For more information, see Configuring an AP as a Sensor on page 178. • Guardian — Applies to AP3710/AP3715/AP376x/AP3825/AP3865/AP3805/AP3801 only. 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 180. 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 472.</p>
Country	Click the country of operation. This option is only available with some licenses. Note: The antenna you select determines the available channel list and the maximum transmitting power for the country in which the AP is deployed.
Professional Install Dialog	
Radio 1 Left Antenna Type	Choose a professional antenna type from the drop-down list for the Radio 1 left antenna, or select No Antenna.
Radio 1 Middle Antenna Type	Choose a professional antenna type from the drop-down list for the Radio 1 middle antenna, or select No Antenna.

Table 13: AP Properties Tab (continued)

Field	Description
Radio 1 Right Antenna Type	Choose a professional antenna type from the drop-down list for the Radio 1 right antenna, or select No Antenna.
Radio 2 Left Antenna Type	Choose a professional antenna type from the drop-down list for the Radio 2 left antenna, or select No Antenna.
Radio 2 Middle Antenna Type	Choose a professional antenna type from the drop-down list for the Radio 2 middle antenna, or select No Antenna.
Radio 2 Right Antenna Type	Choose a professional antenna type from the drop-down list for the Radio 2 right antenna, or select No Antenna.
Radio 1 Attenuation	Choose the desired attenuation for Radio 1 from the drop-down list. Selectable range is from 0 to 30 dBI.
Radio 2 Attenuation	Choose the desired attenuation for Radio 2 from the drop-down list. Selectable range is from 0 to 30 dBI.
Advanced Dialog	
Poll Timeout	<p>Type the timeout value, in seconds. The AP uses this value to trigger re-establishing the link with the IdentifiFi Wireless 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 438.</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@AP 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. • 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 13: AP Properties Tab (continued)

Field	Description
Secure Tunnel Lifetime	<p>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>
Enable SSH Access	<p>Click to enable or disable SSH for access to the AP.</p> <p>Note: The name of this field depends on type of AP that you have selected.</p>
Enable Telnet Access	<p>Click to enable or disable Telnet for access to the AP.</p> <p>Note: The name of this field depends on the type of AP that you have selected.</p>
Enable location-based-service	<p>Enable or disable the AeroScout or Ekahau location-based service for the AP.</p>
Maintain client session in event of poll failure	<p>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.</p>
Restart service in the absence of controller	<p>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.</p>
Use broadcast for disassociation	<p>Select this option if you want the AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This affects the behavior of the AP under the following conditions:</p> <ul style="list-style-type: none"> • If the AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection). • If a BSSID is deactivated or removed on the AP. <p>This option is disabled by default.</p>
Enable LLDP	<p>Click to enable or disable the AP from broadcasting LLDP information. This option is disabled by default.</p> <p>If SNMP is enabled on the controller and you enable LLDP, the LLDP Confirmation dialog is displayed.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> • Proceed (not recommended) — Select this option to enable LLDP and keep SNMP running, and then click OK. • Disable SNMP publishing, and proceed — Select this option to enable LLDP and disable SNMP, and then click OK. • For more information on enabling SNMP, see the Extreme Networks IdentifiFi Wireless <i>Maintenance Guide</i>.

Table 13: AP Properties Tab (continued)

Field	Description
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 applicable to AP36xx, AP37xx, and AP38xx models only and 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>
LED	<p>Select the desired LED pattern from the drop-down list. Options include: Off, WDS Signal Strength, Identify, and Normal.</p>
Real Capture	<p>Click Start to start real capture server on the AP. This feature can be enabled for each AP individually. Statistics are captured using an external connection to a Windows WireShark client. In Wireshark, by selecting the remote APs' IP address and null authentication, the wired and enabled wireless interfaces are listed as available for capture. Default capture server timeout is set to 300 seconds and the maximum configurable timeout is 1 hour. Capture statistics are found on the Active Wireless APs report (see Viewing Statistics for APs on page 505).</p>

Setting Up the Wireless AP Using Static Configuration

Static configuration settings allow you to set up branch office support. These settings can be employed whenever required, and are not dependent on branch topology. In the branch office model, while the controller is at a central office, APs are installed in remote sites. The APs must be able to interact in both the local site network and the central office network. When this is the case, a static configuration is recommended.

For initial configuration of a wireless AP to use a static IP address assignment:

- Allow the AP to first obtain an IP address using DHCP. By default, APs are configured to use the DHCP IP address configuration method.
- Allow the AP to connect to the controller using the DHCP assigned IP address.

- After the AP has successfully registered to the controller, use the **Static Configuration** tab to configure a static IP address for the AP, and then save the configuration.
- Once the static IP address has been configured on the AP, the AP can then be moved to its target location, if applicable.

Note



If a wireless AP with a statically configured IP address (without a statically configured Wireless Controller Search List) cannot register with the controller within the specified number of retries, the wireless AP uses SLP, DNS, and SLP multicast as a backup mechanism.

To Set Up a Wireless AP Using Static Configuration:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate AP in the list.
- 3 Click the **Static Configuration** tab. The Static Configuration page displays.
- 4 Configure the settings on the Static Configuration page, as follows:
 - 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 161. 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 Identifi Wireless *Maintenance Guide*.

- b Select a method of IP address assignment for the AP.

The screenshot shows the configuration interface for a wireless AP. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar shows a list of APs, with 'C4110 - ap3 - AP382' selected. The main content area is titled 'Static Configuration' and contains the following settings:

- VLAN Settings:**
 - Tagged - VLAN ID: (1-4094)
 - Untagged
- IP Address Assignment:**
 - Use DHCP
 - Static Values
- Ethernet Port:**
 - Ethernet Speed:
 - Ethernet Mode:
 - Tunnel MTU:
 - LACP
- Wireless Controller Search List:**
 -
 -
 - Buttons: Up, Down, Delete, Add

At the bottom of the configuration area are buttons for 'Copy to Defaults', 'Reset to Defaults', 'Add Wireless AP', and 'Save'.

Table 14: 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	
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 56). 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 AP 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 Overview on page 112.

Table 14: Static Configuration Properties (continued)

Field/Button	Description
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.
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
Add Wireless AP	Click to manually add and register an AP to the controller
Save	Click to save your changes.

Configuring Telnet/SSH Access

Telnet is used for accessing legacy (non-11n) Access Points. SSH is used for accessing 11n Access Points.



Note

The new telnet/SSH access password that you set up over the controller's user interface overrides the default access password. The process for setting up the new password is described below.

To enable or disable telnet or SSH access:

- 1 From the top menu, click **AP**. The Wireless APs screen displays.
- 2 In the AP list, click the AP for which you want to enable or disable telnet.
- 3 Click **Advanced**. The Advanced dialog is displayed.
- 4 In the **Telnet Access/SSH Access** drop-down list, click one of the following:
 - **Enable** – Enables telnet/SSH access
 - **Disable** – Disables telnet/SSH access



Note

The option to enable or disable telnet access or SSH access is displayed only if the wireless AP is a legacy AP. For 11n wireless APs, SSH is always enabled by default.

- 5 To save your changes, click **Save**.
- To set up a new telnet/SSH access password:
- 6 From the top menu, click **AP**. The **Wireless APs** screen displays.

- 7 In the left pane, click **Global Settings > AP Registration**. The **Wireless AP Registration** screen displays.



Note

The SSH Access section on the AP Registration screen is applicable to the 11n wireless APs. The Telnet Access section is applicable to the legacy APs.

- 8 If you are setting up a new telnet access password for a legacy AP, type the new password in the **Password** box under the **Telnet Access** section. If you are setting up a new SSH access password for an 11n AP, type the new password in the **Password** box under the **SSH Access** section.
- 9 In the **Confirm Password** box, re-type the password.
- 10 To save your changes, click **Save**.

Configuring Wireless AP Radio Properties

Wireless AP radio properties can vary significantly 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 149.
- For specific information on modifying a legacy (pre-11n) wireless AP, see [Modifying Legacy Wireless AP Radio Properties](#) on page 154.

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 504.

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 Identifi Wireless AP36xx/37xx/W78xC series are 802.11n-compliant access points. AP38xx series are 11n and 11ac-compliant. This section describes how to configure/modify properties of an 11n or 11ac AP.

For information on how to modify a legacy (pre-11n) wireless AP, see [Modifying Legacy Wireless AP Radio Properties](#) on page 154.

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. To achieve a 40 MHz channel width, the 802.11n AP employs channel bonding — two 20 MHz channels at the same time.

The 40 MHz channel width is achieved by bonding the primary channel (20 MHz) with an extension channel that is either 20 MHz above (bonding up) or 20 MHz below (bonding down) of the primary 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 frequency can use 40 MHz, 20 MHz, or the 802.11a/b/g radio protocols.

- 802.11n clients that do not support the 40 MHz frequency 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 frequency 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 frequency 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 and 40 MHz, depending on how busy the extension channel is. 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. Depending on the primary channel that is selected, channel bonding may be allowed: up or down.

Guard Interval

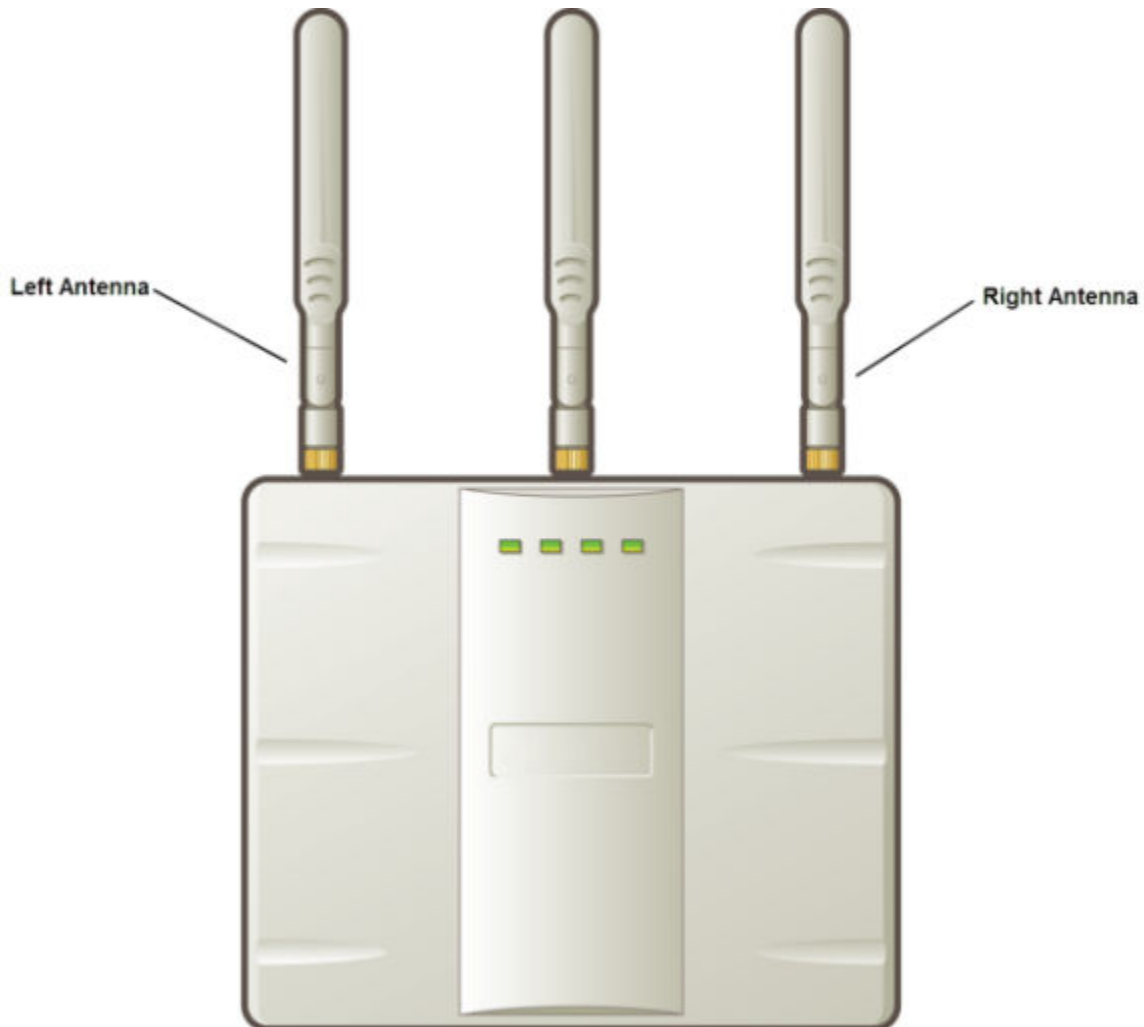
The guard intervals ensure that individual transmissions do not interfere with one another. The wireless 802.11n AP provides a shorter guard interval that increases the channel throughput. When a 40 MHz channel is used, you can select the guard interval to improve the channel efficiency. The guard interval 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. The AP3620, for example, has three antennas: left, middle, and right. The illustration below identifies the left and right antennas for the AP3620.



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 802.11n AP to transmit on specific antennas for both radios, including all the available modes:

- **Radio 1** – a, a/n, a/n/ac, ac-strict modes
- **Radio 2** – b, b/g, b/g/n, g, 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**. The **Wireless AP** screen displays.
- 2 Click the appropriate wireless AP in the list. The **AP Properties** tab is displayed.
- 3 Click the **Radio** tab you want to modify.

Achieving High Throughput with 11n and 11ac Wireless APs

To achieve link rates of up to 300 Mbps, 450 Mbps, or 1.3 Gbps with the 36xx, 37xx and 38xx series wireless APs, configure your system as described in this section.



Note

Maximum throughput cannot be achieved if both 802.11n and legacy client devices are to be supported.



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**. The **AP** screen displays.
- 2 In the left pane click on the **APs** button, then in the **AP** list, click the AP you want to configure.
- 3 Click the **Radio 2** tab, and then do the following:
 - In the **Radio Mode** drop-down list, click b/g/n.
 - In the **Channel Width** drop-down list, click 40 MHz.



Note

Some client devices do not support 40 MHz in b/g/n mode. To accommodate these clients, enable a/n mode on the **Radio 1** tab. Otherwise, the client device connects at 130Mbps only.

- 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 AP3825 enter 1048575)
- **Agg. MPDUs Max # of Sub-frames** — Type **64**.
- **ADDBA Support** — Click **Enabled**.

- 4 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 AP3865, click a/n/ac).
 - In the **Channel Width** drop-down list, click **40 MHz** (for the AP3825 and AP3865, 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**.
- 5 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 6 In the left pane **Virtual Networks** list, click the VNS to configure. The **Topology** tab is displayed.
- 7 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.

- 8 Click the **QoS Role** tab.
- 9 In the **Wireless QoS** section, select the **WMM** option. Some 802.11n client devices remain at 54Mbps unless WMM is enabled.

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 243.

**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 290.

- **AP Multi-edit** — When you configure multiple APs simultaneously, use the AP Multi-edit feature. For more information, see [Configuring Multiple Wireless APs Simultaneously](#) on page 109.
- **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 Individual AP:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate AP in the list. The **AP Properties** tab is displayed.
- 3 Click the **WLAN Assignment** tab.

The screenshot shows the 'AP Properties' screen with the 'WLAN Assignment' tab selected. The interface includes a top navigation bar with 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. On the left, there is a list of APs under the heading 'APs', with 'C4110 - ap3 - AP382' selected. The main area displays a table with columns for 'WLAN Name', 'Radio 1', and 'Radio 2'. Below the table are buttons for 'Copy to Defaults', 'Reset to Defaults', 'Add Wireless AP', and 'Save'.

WLAN Name	Radio 1	Radio 2
CNL-422-0-0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CNL-422-0-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CNL-422-0-2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CNL-422-0-3	<input checked="" 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 checked="" type="checkbox"/>	<input type="checkbox"/>
CNL-422-1-6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CNL-422-1-7	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CNL-422-2-10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CNL-422-2-11	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CNL-422-2-12-wds	<input type="checkbox"/>	<input type="checkbox"/>
CNL-422-2-8	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CNL-422-2-9	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CNL-422-3-12	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CNL-422-3-13	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

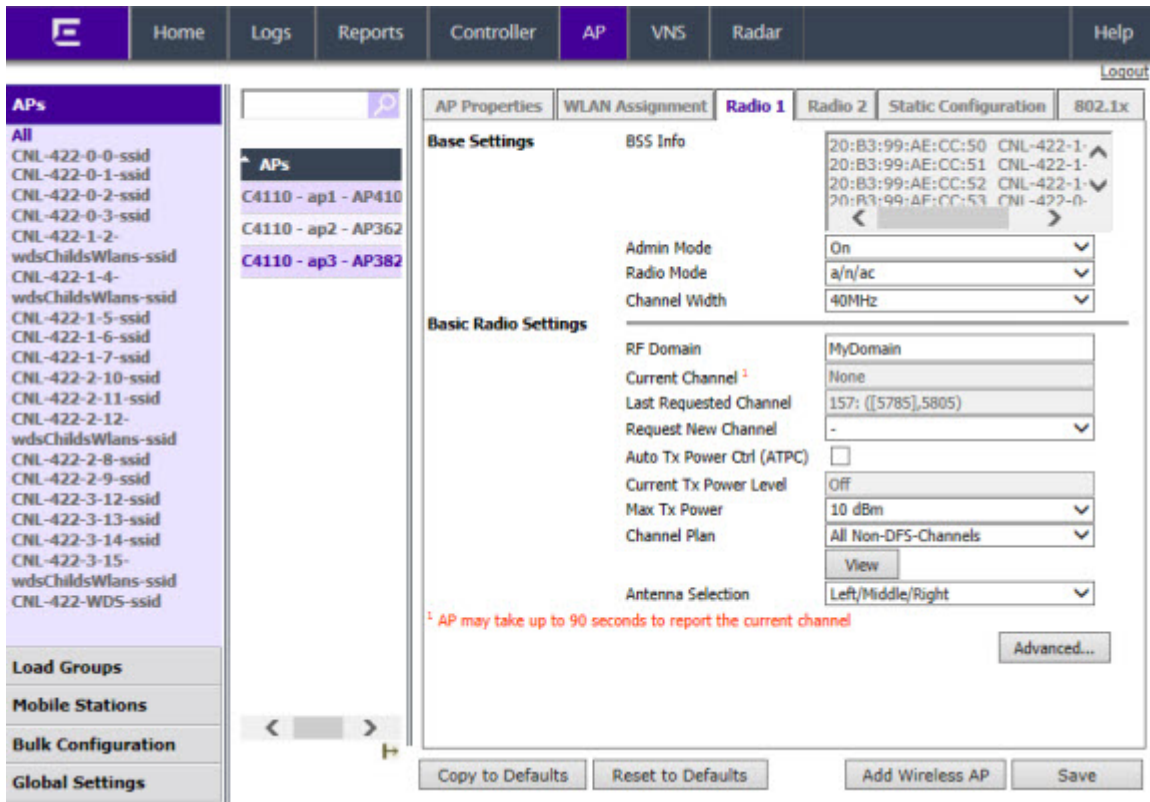
Modifying Legacy Wireless AP Radio Properties

The following section describes how to modify a legacy AP (2610/2620 and the AP2650/2660). For information on how to modify an 11n AP (36xx/37xx/38xx/W78xC), see [Modifying 11n and 11ac Wireless AP Radio Properties](#) on page 149.

To modify a legacy Wireless AP's radio properties:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 Click the appropriate legacy AP in the list. The **AP Properties** tab is displayed.

- 3 Click the **Radio** tab you want to modify. For more information on all Radio parameters, see [Configuration Parameters for Radio Properties](#) on page 155.



Configuration Parameters for Radio Properties

Table 15: Radio Properties

Field	Description
Base Settings	
BSS Info	BSS Info is read-only. After WLAN Service configuration, the Basic Service Set (BSS) section displays the MAC address on the AP for each WLAN Service and the SSIDs of the WLAN Services to which this radio has been assigned.
Admin Mode	Select On to enable the radio; select Off to disable the radio.

Table 15: Radio Properties (continued)

Field	Description
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.
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 147).
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.

Table 15: Radio Properties (continued)

Field	Description
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 632.</p>
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>

Table 15: Radio Properties (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. 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>
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.

Radio Advanced Properties

Table 16: Advanced Radio Properties

Field	Description
Advanced Dialog - Base Settings	
DTIM period	Type the desired DTIM (Delivery Traffic Indication Message) period — the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. Use a small number to minimize broadcast and multicast delay. The default value is 5.
Beacon Period	Type the desired 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. This setting is not applicable for the AP3825 or AP3865 radio. 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"> • Off — Disables the feature • 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 and AP38xx series APs.

Table 16: 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	
Protection Mode	Click a protection mode: None, Auto, or Always. The default and recommended setting is Auto. Click None if 11b APs and clients are not expected. Click Always if you expect many 11b-only clients.
Extension Channel Busy Threshold	Click a protection type, CTS Only or RTS CTS, when a 40 MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
Aggregate MSDUs	Click an aggregate MSDU mode: Enabled or Disabled. Aggregate MSDU increases the maximum frame transmission size.
Aggregate MPDUs	Click an aggregate MPDU mode: Enabled or Disabled. Aggregate MPDU provides a significant improvement in throughput.
Aggregate MPDU Max Length	Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes. For the 802.11ac radio (Radio 1 of the AP38xx), the range is 1024-1048575.
Agg. MPDU Max # of Sub-frames	Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
ADDBA Support	Click an ADDBA support mode: Enabled or Disabled. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. ADDBA Support must be enabled if Aggregate APDU is enable.
LDPC	Click an LDPC mode: Enabled or Disabled. LDPC increases the reliability of the transmission resulting in a 2dB increased performance compared to traditional 11n coding.
STBC	Click an STBC mode: Enabled or Disabled. STBC is a simple open loop transmit diversity scheme. When enabled, STBC configuration is 2x1 (two spatial streams combine into one spatial stream). TXBF overrides STBC if both are enabled for single stream rates.

Table 16: Advanced Radio Properties (continued)

Field	Description
TXBF	Click an TXBF mode: Enabled or Disabled. 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.
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.

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**. The **Wireless APs** screen displays.
- 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.

Configuring 802.1x 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.

To Configure 802.1x PEAP Authentication:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the APs list, click the AP for which you want to configure 802.1x PEAP authentication.
- 3 Click the **802.1x** tab.

The screenshot shows the configuration interface for a wireless AP. The top navigation bar includes Home, Logs, Reports, Controller, AP (selected), VNS, Radar, and Help. The left sidebar lists various APs under the 'APs' section, with 'C4110 - ap2 - AP362' selected. The main content area is titled '802.1x' and contains the following sections:

- Certificate status:** A section with a 'Generate Certificate Signing Request' button.
- Authentication methods:**
 - EAP-TLS:** Includes fields for 'X509 DER / PKCS#12 file:' (with a 'Browse...' button) and 'Password:'. A 'Delete EAP-TLS credentials' button is located below.
 - PEAP:** Includes dropdown menus for 'Username:' (set to '-no change-') and 'Password:' (set to '-no change-'). A 'Delete PEAP credentials' button is located below.
- Current Credentials:** A section with a dropdown menu.

At the bottom of the configuration area, there are buttons for 'Copy to Defaults', 'Reset to Defaults', 'Add Wireless AP', and 'Save'.

- In the **Username** drop-down list, click the value you want to assign as the user name credential:

Table 17: 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.

- In the **Password** drop-down list, click the value you want to assign as the password credential (see [Table 17: Credential Parameters](#) on page 164 for credential parameters and values).
- 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.

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 164
- [Pass Through Mode](#) on page 165



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:

- From the top menu, click **AP**. The **AP** screen displays.
- In the AP list, click the wireless AP for which you want to configure 802.1x EAP-TLS authentication.
- Click the **802.1x** tab.
- Click **Generate Certificate Signing Request**. The **Generate Certificate Signing Request** window is displayed.

- 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 17: Credential Parameters](#) on page 164 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** window 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**. The **AP** screen displays.
- 2 In the AP list, click the AP for which you want to configure 802.1x EAP-TLS authentication.
- 3 Click the **802.1x** tab.
- 4 Click **Browse**. The **Choose file** window is displayed.
- 5 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.
- 6 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.

- 7 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**. The **AP** screen displays.
- 2 In the AP list, click the wireless AP 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.

Extreme networks **Wireless AP Credentials**

Current credentials in use by Wireless AP

PEAP

Username: 0500008023050025

Password: [Masked]

EAP-TLS Certificate

Serial number: 323EC870000000000015C

Expiry date: Thursday, April 05th, 2012, 02:17:28 PM

Issued on: Wednesday, April 06th, 2011, 02:17:28 PM

Issuer: CN=testypc, DC=com

Full subject distinguished name: CN=Users, CN=AP1 Credential, DC=com,

Subject alternative name: Principal Name=ap_admin

Close

Deleting 802.1x Credentials



Caution

Exercise caution when deleting 802.1x credentials. For example, deleting 802.1x credentials may prevent the AP from being authenticated or cause it to lose its connection with the controller.

To Delete Current 802.1x Credentials:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Bulk Configuration**, then in the AP list, click the AP for which you want to delete its current 802.1x credentials.

- 3 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 Multi-edit

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.
- 2 In the left pane, click **Bulk Configuration > AP 802.1x Multi-edit**.

The screenshot shows the AP configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP (selected), VNS, Radar, and Help. The left sidebar shows the navigation menu with 'Bulk Configuration' selected, and 'AP 802.1x Multi-edit' highlighted. The main content area displays the '802.1x Authentication' settings for multiple APs. The settings are organized into three sections: Certificate Signing Request, Bulk Certificate Upload, and PEAP Authentication. The Certificate Signing Request section includes fields for Country name, State or Province name, Locality name (city), Organization name, Organizational Unit name, Common name (set to MAC), and Email address. The Bulk Certificate Upload section includes a field for PFX, CER or ZIP File (with a Browse... button) and a Password field. The PEAP Authentication section includes fields for Username (set to MAC) and Password (set to MAC). A red note at the bottom states: 'Uploading single zipped certificate to multiple APs is not supported.'

- 3 In the **APs** list, click one or more APs to configure. To select multiple APs, click the APs from the list while pressing the CTRL key. To search for a specific AP, enter the AP in the search bar and click .
- 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 17: Credential Parameters](#) on page 164 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** window 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.

To Configure 802.1x EAP-TLS Authentication in Pass Through Mode Using Multi-edit:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Bulk Configuration** > AP 802.1x Multi-edit.
- 3 In the **APs** list, click one or more APs to configure. To select multiple APs, click the APs from the list while pressing the CTRL key.
- 4 In the **Bulk Certificate Upload** section, click **Browse**. The **Choose file** window is displayed.
- 5 Navigate to the location of the file (.zip or .pfx), and then click **Open**. The name of the file is displayed in the **PDFX, CER or ZIP Archive** box.
- 6 In the **Password** box, type the password used during the certificates generation process.
- 7 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.

To Configure 802.1x PEAP Authentication Using Multi-edit:

- 8 From the top menu, click **AP**. The **AP** screen displays.
- 9 In the left pane, click **Bulk Configuration** > **AP 802.1x Multi-edit**.
- 10 In the **Wireless APs** list, click one or more APs to edit. To select multiple APs, click the APs from the list while pressing the CTRL key.
- 11 In the **PEAP** Authentication section, do the following:
 - In the Username drop-down list, click the value you want to assign as the user name credential (see [Table 17: Credential Parameters](#) on page 164 for credential parameters and values).
 - In the Password drop-down list, click the value you want to assign as the password credential (see [Table 17: Credential Parameters](#) on page 164 for credential parameters and values).
- 12 Click **Set PEAP credentials**. The **AP 802.1x Multi-edit progress** window is displayed, which provides the status of the configuration process. Once complete, the **Settings updated** message is displayed in the footer of the Wireless Assistant.

The 802.1x PEAP authentication configuration is assigned to the APs. The APs can now be deployed to 802.1x enabled switch ports.

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 18: Maximum Number of Load Balance Groups

IdentifiFi Wireless Appliance	Number of load balance groups
C4110	32
C5110	64
C5210	64
C25	8
C35	8
V2110	64

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

- AP3801i
- AP3805 (i & e)
- AP3825 (i & e)
- AP3865e
- AP3765/67

- AP3705i
- AP3710 (i & e)
- AP3715 (i & e)
- AP3605
- AP3610
- AP3620
- AP3630 (in fit mode only)
- AP3640 (in fit mode only)
- AP3660

To create a load balance group, see [Creating a Load Balance Group](#) on page 172.

Creating a Load Balance Group

To create a load balance group:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Load Groups**.

The **Wireless AP Load Groups** page displays.

Name	Type	APs Assigned	WLANs Assigned
CNL-208-1	Client Balancing	0	0
CNL-208-2	Radio Preference	0	0
CNL-208-3	Radio Preference	0	0
CNL-208-4	Radio Preference	0	0

- 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.

Radio 1(Available †)	Radio 2(Available †)	AP Name
<input type="checkbox"/> a/n(5)	<input type="checkbox"/> b/g/n(6)	C4110 - ap2 - AP3620
<input type="checkbox"/> a/n/ac(1)	<input type="checkbox"/> b/g/n(1)	C4110 - ap3 - AP3825e

† # of VNS available for load group WLAN Assignment for the radio.

If you are adding a Radio Preference load balancing group, the **Radio Preference** tab becomes available.

Load Group ID: 125 Type: Radio Preference

Radio Preference **WLAN Assignment**

Band Preference
Enable:

Load Control

	Enable	Max # of Clients	Strict Limit
Radio1	<input type="checkbox"/>	112	<input type="checkbox"/>
Radio2	<input type="checkbox"/>	112	<input type="checkbox"/>

AP Assignment:

AP Name(Radio 1 Available †, Radio 2 Available †)	
C4110 - ap2 - AP3620(5,6)	<input type="checkbox"/>
C4110 - ap3 - AP3825e(1,1)	<input type="checkbox"/>

† # of VNS available for load group WLAN Assignment for the radio.

New Delete Save

The radios for both types of load groups can be assigned to a WLAN, on the **WLAN Assignment** tab.

Radio Assignment **WLAN Assignment**

WLAN Name	
cp	<input type="checkbox"/>
Lab126-13-AAA	<input type="checkbox"/>

New Delete Save



Note

For more information about the fields on these screens, see [Configuration Parameters for AP Load Groups](#) on page 175

Configuration Parameters for AP Load Groups

Table 19: 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.
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 - this tab is available only for load groups assigned the Client Balancing type	
Select AP Radios	From the drop-down menu, select the AP radios that you want to assign to the load group. Options include: <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 - this tab is available only for load groups assigned the Radio Preference type	
Band Preference	Select the Enable checkbox to enable band preference for this load group. <p>For the AP36xx models only, you can apply band preference only 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 reassociate with an 11g radio, it is rejected if the AP determines that the client is 11a capable.</p>

Table 19: AP Load Groups (continued)

Field/Button	Description
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.
WLAN Assignment tab	
WLAN Name	<p>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.</p> <p>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.</p>

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 432.

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 509.

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 AP's in the Site

APs operating on the same subnet with multicast and IGMP 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 AP's 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**. The **AP** screen displays.

- 2 In the left pane, click **Global Settings**, then **AP Registration**. The **AP Registration** screen displays.

- 3 In the **Secure Cluster** section, enter a cluster shared secret.
- 4 Enable cluster encryption by clicking on the **User Cluster Encryption** checkbox. APs on which user cluster encryption is disabled cannot participate in the cluster.
- 5 Enable or disable support for inter-AP roaming by clicking on the **Inter AP Roam** checkbox.
- 6 Click **Save**.

Configuring an AP as a Sensor



Note

APs of the 37xx and 38xx series cannot be converted to use as sensors for WAS. This section applies to APs in the 36xx and 26xx series only.

Wireless 36xx and 26xx access points that are configured as sensors perform scanning services and relay information to Wireless Advanced Services (WAS). WAS provides monitoring, administration, troubleshooting, and protection services for your wireless network.

When an AP is Approved as Sensor:

- The AP severs its connection to the controller
- The AP registers with Wireless Advanced Services (WAS)
- The AP performs scanning services
- The AP no longer performs RF services for the controller

The following wireless APs have sensor capability:

- AP2610/AP2620
- AP2630/AP2640
- AP3610/AP3620
- AP3630/AP3640
- AP3660

**Note**

APs 2630/2640 and 3630/3640 have to be converted to fit mode and connected to a controller before being converted to a sensor.

When an AP is operating as a sensor, it has no interaction with the controller, and it does not perform like an AP. It does not allow devices to associate to it and traffic is not forwarded through it. An AP operating as a sensor is managed by Wireless Advanced Services (WAS). The WAS sensor domain license (SDL) limit governs the number of sensors a customer can have.

When an AP is configured as a sensor, the AP's current configuration is retained in the controller database. If the sensor is later configured back to perform RF services, its previous configuration data is reassigned to it.

Before APs can be configured as sensors, first download the sensor image from a TFTP server to the controller:

To Download the WAS Sensor Image from a TFTP Server to the controller:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **WAS > Sensor Management**. The **WAS Sensor Management** screen displays.

- 3 In the **Local Sensor Images** field, select AP26xx or AP36xx.

- 4 In the **Download Sensor Images** field, type the following:
 - **Sensor Platform** - Select an AP type from the drop-down list.
 - **TFTP Server** – The IP address of the TFTP server the AP is to retrieve the sensor image file from.
 - **Directory** – The location of the AP26xx or AP36xx sensor image on the TFTP server.
 - **Filename** – The filename of the AP26xx or AP36xx sensor image on the TFTP server.
- 5 Click **Download**.
- 6 Once you have downloaded the sensor image, configure the appropriate wireless AP as a sensor from either the **Wireless APs All APs** screen or the **Wireless APs Access Approval** screen.

To configure the wireless AP as a sensor from the **Wireless APs All APs** screen:

 - a From the top menu, click **AP**. The AP screen displays.
 - b In the AP list, click the AP whose properties you want to modify. The **AP Properties** tab displays AP information.
 - c Select the AP that you want to configure as a sensor.
 - d In the Role field, select **Sensor**.
 - e Click Save.

To configure the wireless AP as a sensor from the **Wireless APs Access Approval** screen:

 - f From the top menu, click **AP**. The AP screen displays.
 - g In the left pane, click **Bulk Configuration > Access Approval**. The **Access Approval** screen displays, along with the registered APs and their status.
 - h Select the checkbox next to the wireless AP that you want to configure as a sensor.
 - i Click **Sensor**.

Configuring an AP as a Guardian



Note

This section applies to the AP3710, AP3715, AP376x, AP3805, AP3801, AP3825, and AP3865 series only.

Wireless 3710, 3715, 376x, 3801, 3805, 3825, 3865 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.

The following wireless APs have guardian capability:

- AP3801i
- AP3710i
- AP3710e
- AP3715i
- AP3715e
- AP376x

- AP3805
- AP3825i
- AP3825e
- AP3865e

To Configure an AP as a Guardian Scan Profile:



Note

Once an AP is assigned to a Guardian Scan Profile it will stop forwarding traffic on both radios.

- 1 From the top menu, click **Radar**. The **Radar** screen displays.
- 2 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.

The screenshot shows the Radar configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar shows Configuration, Scan Profiles, Legacy Scan, In-Service Scan, Guardian Scan, Maintenance, and Location Engine. The main area displays the Scan Profiles table with the following data:

Name	Profile	Type	Security Scan	Interference Scan	Status
<input type="checkbox"/> smokeTestScanC4110	Legacy	Active	×	N/A	Disabled

An "Add Scan Profile" dialog box is open, showing a "Profile" dropdown menu set to "Guardian". The dialog also includes "Add" and "Cancel" buttons.

- 5 Click **Add**. For more information, see [Configuring a Guardian Scan Profile](#) on page 472.

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.



Note

The controller does not ship with sensor software. Download sensor software from a TFTP server to the local controller.

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**. The **Wireless APs** screen displays.
- 2 In the left pane, click **Global Settings**, then **AP Maintenance**. The **AP Software Maintenance** tab is displayed.

The screenshot shows the 'AP Software Maintenance' configuration page. The top navigation bar includes Home, Logs, Reports, Controller, AP (selected), VNS, Radar, and Help. A 'Logout' link is visible in the top right. The left sidebar shows a tree view with 'Global Settings' selected, containing 'AP Maintenance', 'AP Registration', and 'WAS Sensor Management'. The main content area is titled 'AP Software Maintenance' and has a sub-tab 'AP Maintenance Cycle'. It features an 'AP Images for Platform:' dropdown menu set to 'AP2600', displaying a list of images with 'AP200-09.21.01.0160.img (Default)' selected. Below the list are 'Set as default' and 'Delete' buttons. To the right, the 'Download AP Images:' section includes input fields for 'FTP Server', 'User ID', 'Password', 'Confirm', 'Directory', and 'Filename', along with a 'Platform:' dropdown set to 'AP2600' and a 'Download' button. The 'Upgrade Behavior:' section has two radio buttons: '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, it shows 'Disk space left for images: 13143 MB' and a 'Save' button.

- 3 In the **AP Images for Platform** drop-down list, click the appropriate platform.

- 4 To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.
- 5 In the **Upgrade Behavior** section, select one of the following:
 - Upgrade when AP connects using settings from Controlled Upgrade — The **Controlled Upgrade** tab is displayed when you click **Save**. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.
 - Always upgrade AP to default image (overrides Controlled Upgrade settings) — Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.
- 6 To save your changes, click **Save**.

Scheduling a Maintenance Cycle for Specific APs

To Schedule a Maintenance Cycle for Specific APs

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Global Settings**, then **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
- 3 Click the **AP Maintenance Cycle** tab.

- 4 Under **Schedule**, click the **Start At** box. The **Choose Time** dialog appears.
- 5 In the **Choose Time** dialog, 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**.
- 10 From the top menu, click **AP**. The **AP** screen displays.
- 11 In the left pane, click **Global Settings**, then **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
- 12 In the **AP Images for Platform** drop-down list, click the appropriate platform.
- 13 In the **AP Images** list, click the image you want to delete.
- 14 Click **Delete**. The image is deleted.

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 Settings**, then **AP Maintenance**. The **AP Software Maintenance** tab is displayed.
- 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**. The **AP** screen displays.
- 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**. The **AP** screen displays.
- 2 In the left pane, click **AP Maintenance**. The **AP Software Maintenance** tab is displayed.

- Click the **Controlled Upgrade** tab.

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.

- In the **Select AP Platform** drop-down list, click the type of AP you want to upgrade.
- In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.
- In the list of registered **Wireless APs**, select the checkbox for each AP to be upgraded with the selected software image.
- Click **Apply AP image version**. The selected software image is displayed in the **Upgrade To** column of the list.
- To save the software upgrade strategy to be run later, click **Save for later**.
- 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 IdentifiFi Wireless AP 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:

- [38xx Series Wireless APs](#) on page 186
- [37xx Series Wireless APs](#) on page 190
- [36xx 11n Wireless APs](#) on page 194
- [26xx and Other Legacy Wireless APs](#) on page 199

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 207.

38xx Series Wireless APs

WS-AP3801i LED Indicators

The WS-AP3801i provides three LED indicators (see [Figure 12: AP3801i Top View](#) on page 186). The LEDs provide status information (see [Table 20: AP3801i LED Status Indicators](#) on page 186) on the current state of the WS-AP3801i.

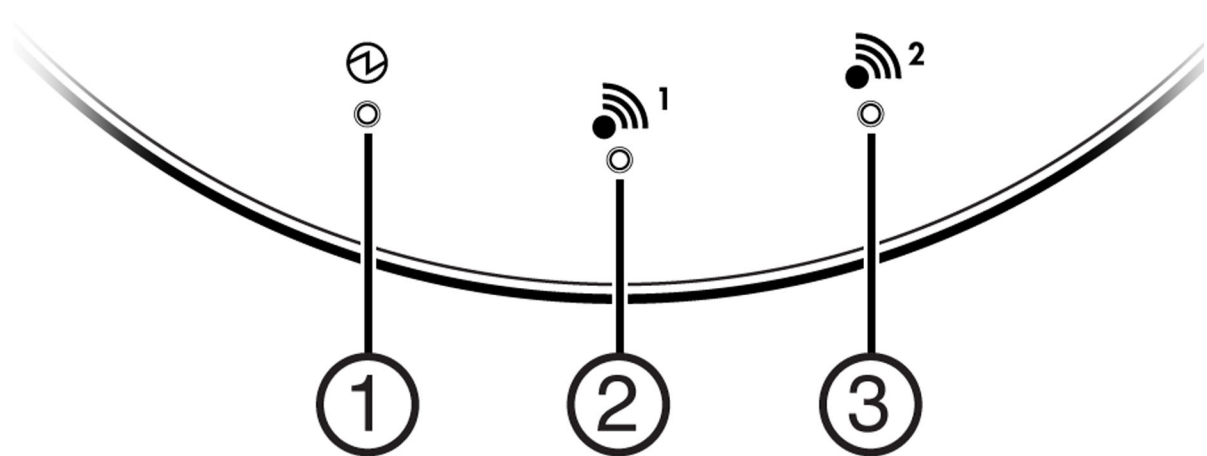


Figure 12: AP3801i Top View

Table 20: 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 13: AP3805i/e Top View](#) on page 187). The LEDs provide status information (see [Table 21: AP3805i/e LED Status Indicators](#) on page 187) on the current state of the WS-AP3805i/e.

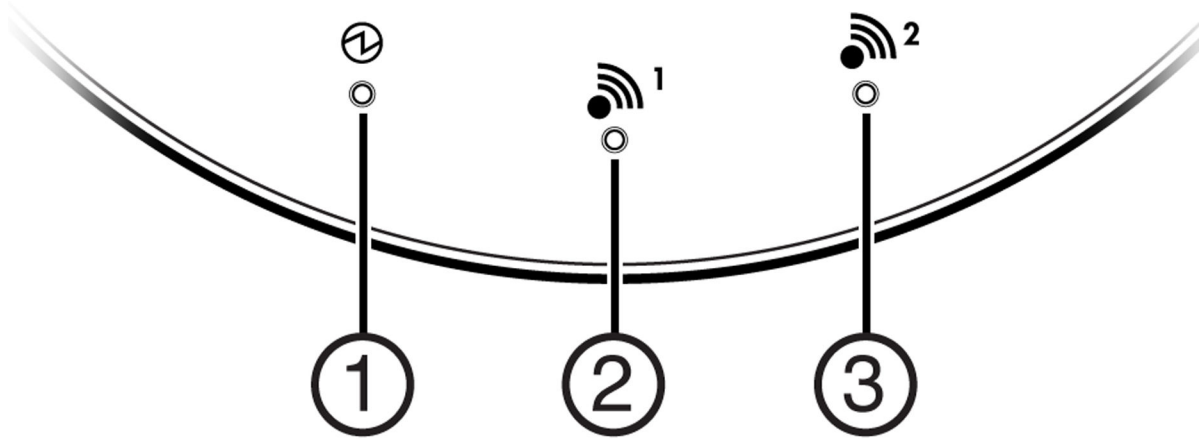


Figure 13: AP3805i/e Top View

Table 21: 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.
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 [Figure 14: WS-AP3865e LEDs](#) on page 188 below. The LEDs provide status information, described in [Table 22: WS-AP3865 LED Indications](#) on page 188, on the current state of the WS-AP3865e.

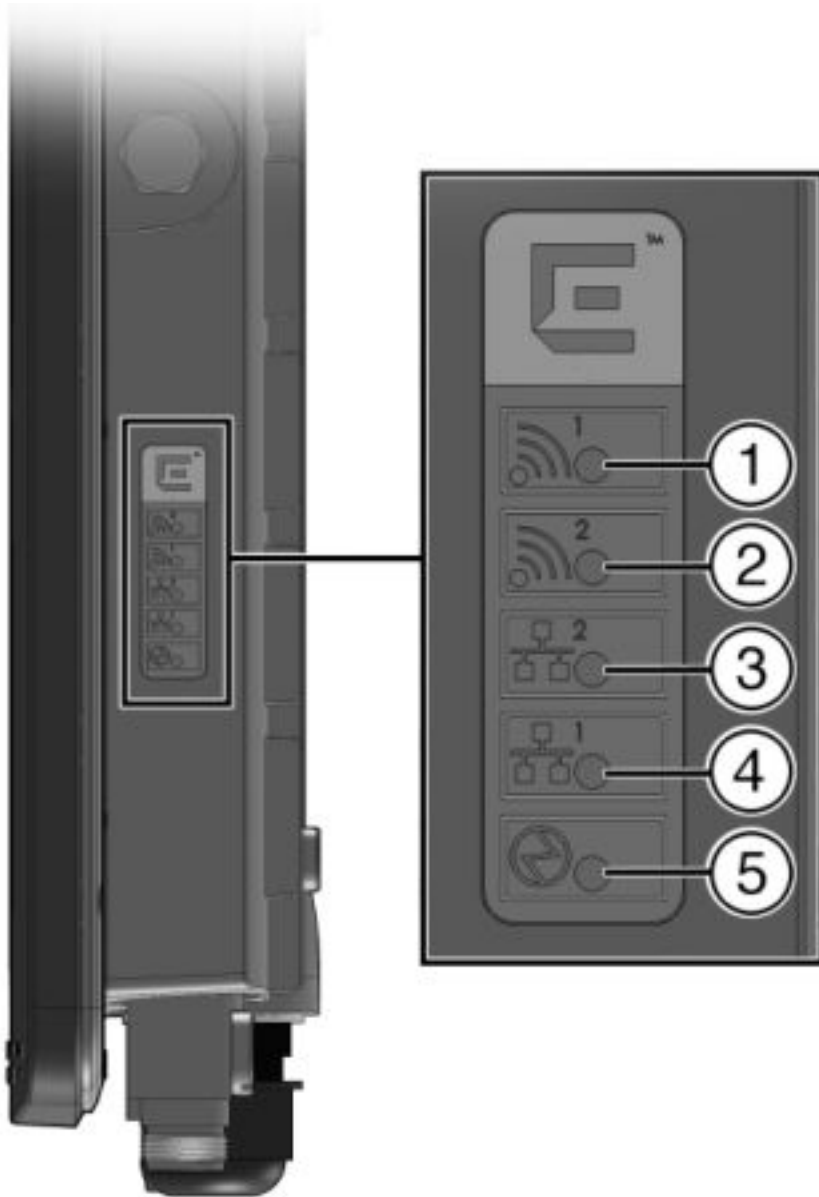


Figure 14: WS-AP3865e LEDs

Table 22: 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.

Table 22: WS-AP3865 LED Indications (continued)

LED	Status	Description
	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 [Figure 15: WS-AP3825 LEDs](#) on page 189 below. The LEDs provide status information, described in [Table 23: WS-AP3825 LED Indications](#) on page 190, on the current state of the WS-AP3825.

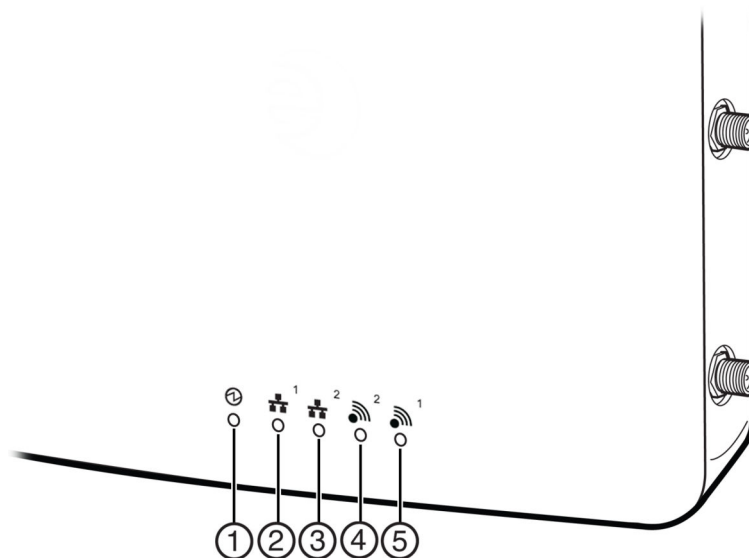


Figure 15: WS-AP3825 LEDs

Table 23: 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 IdentifiFi Wireless 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 191
- [WS-AP3715 LED Indicators](#) on page 192
- [AP3765/AP3767/W786C LED Status](#) on page 194

WS-AP3705i LED Indicators

The WS-AP3705i provides four LED indicators (see [Figure 16: AP3705i Top View](#) on page 191). The LEDs provide status information (see [Table 24: AP3705i LED Status Indicators](#) on page 191) on the current state of the WS-AP3705i.

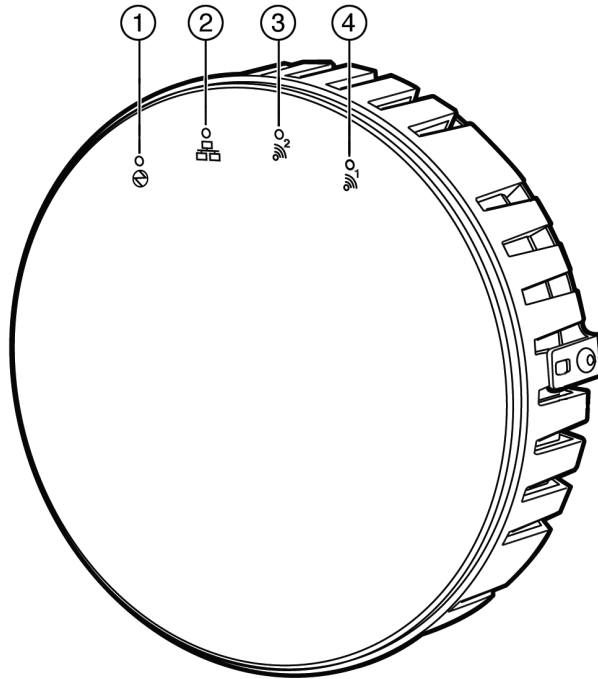


Figure 16: AP3705i Top View

Table 24: 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 [Figure 17: WS-AP3710 LEDs \(Front, lower right\)](#) on page 192 below. The LEDs provide status information, described in [Table 25: WS-AP3710 LED Indications](#) on page 192, on the current state of the WS-AP3710.

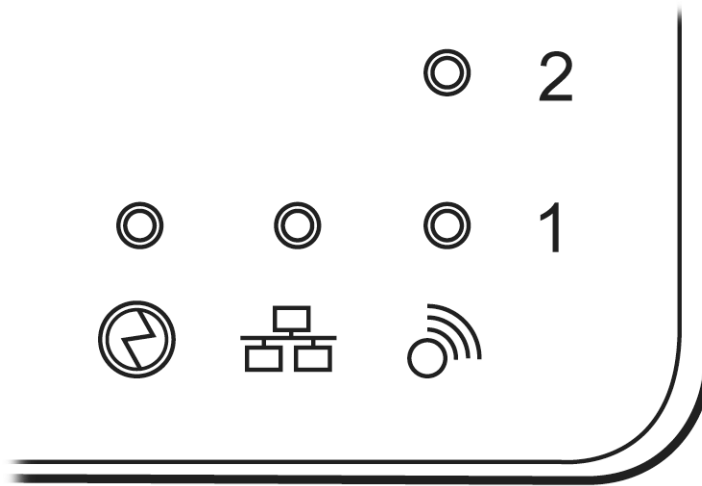


Figure 17: WS-AP3710 LEDs (Front, lower right)




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

Table 25: 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 [Figure 18: WS-AP3715 LEDs](#) on page 193 below. The LEDs provide status information, described in [Table 26: WS-AP3715 LED Indications](#) on page 193, on the current state of the WS-AP3715.

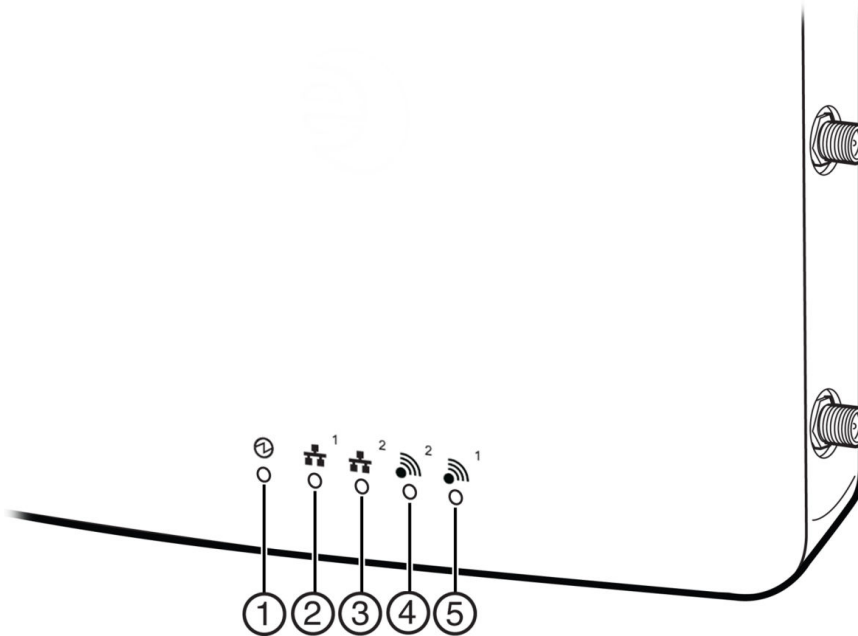


Figure 18: WS-AP3715 LEDs




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

Table 26: 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 IdentifiFi Wireless 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 ([Figure 19: Extreme Networks Wireless Outdoor AP3765/AP3767/W786C LEDs](#) on page 194) displays six LEDs. These LEDs provide information on operating status.

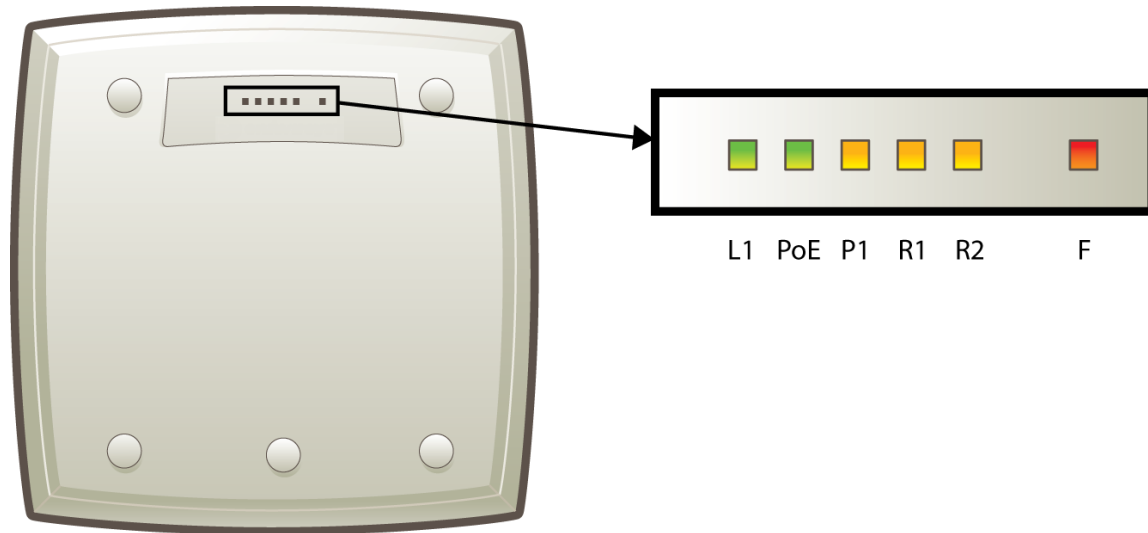


Figure 19: Extreme Networks Wireless Outdoor AP3765/AP3767/W786C LEDs

Table 27: 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.

36xx 11n Wireless APs

The IdentifiFi Wireless AP36xx product series are 802.11n APs that are also compatible with earlier 802.11a/b/g protocols. The LED indicators on these are described in the following subsections:

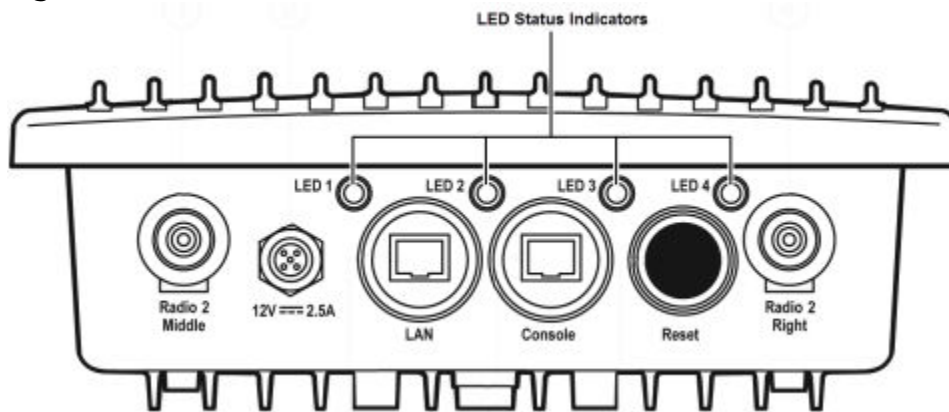
- [Extreme Networks Wireless Outdoor AP3660 LED Indicators](#) on page 195

- [IdentifiFi Wireless AP3610, AP3620 LED Status](#) on page 196

Extreme Networks Wireless Outdoor AP3660 LED Indicators

The AP3660 provides four LED indicators (see [Figure 20: AP3660 Bottom View](#) on page 195). The LEDs provide status information (see [Table 28: AP3660 LED Status Indicators](#) on page 195) on the current state of the AP3660.

Figure 20: AP3660 Bottom View



Note



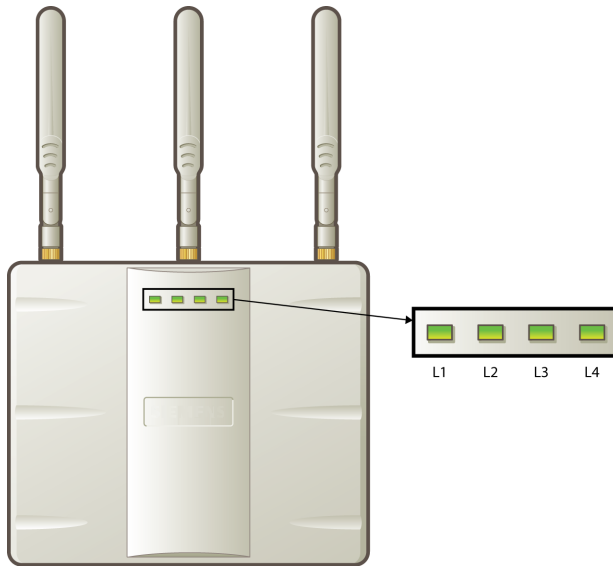
The AP3660 provides six external antenna ports. The network administrator determines which antenna port will be used based on the external antenna selected. The AP3660 can also be configured to select the antenna that provides the best possible data transmission (diversity).

Table 28: AP3660 LED Status Indicators

LED	Status	Description
1 (Power)	On Green	Indicates the AP3660 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.
	On Red	Indicates a valid 10Mbps Ethernet link.
3 (Wireless Link)	On Green	Indicates Radio 1 (5 GHz) is enabled.
	Flashing Green	Indicates the AP3660 is transmitting or receiving data.
4 (Wireless Link)	On Green	Indicates Radio 2 (2.4 GHz) is enabled.
	Flashing Green	Indicates the AP3660 is transmitting or receiving data.

IdentifiFi Wireless AP3610, AP3620 LED Status

Figure 21: IdentifiFi Wireless AP3610/3620 LEDs on page 196 depicts the location of the LEDs on the IdentifiFi Wireless AP3610/3620.



LEDs L1, L3, and L4 work in conjunction to indicate the general, high-level, and detailed state respectively. LED L2 indicates the status of the Ethernet port.

After initialization and discovery is completed and the AP is connected to the IdentifiFi Wireless Controller, LEDs L3 and L4 indicate the state of the corresponding radio — L3 for Radio 5 GHz, and L4 for Radio 2.4 GHz.

Figure 21: IdentifiFi Wireless AP3610/3620 LEDs

LEDs Color Codes

The AP3610/3620 LEDs indicate “normal-operation”, “warning/special”, or “failed” state of the Wireless AP in the following color codes:

Table 29: AP3610/3620 LED Color Codes

LED Color/State	Description
Green	Normal operational state.
Orange/amber	Warning or special state, such as WDS.
Blinking	AP state, such as initialization or discovery, is in progress.
Red	Error state
Steady color	AP state is stable; process is completed. For example, initialization is finished or discovery completed.

LED L1

LED L1 indicates the general state of the AP3610/3620:

Table 30: LED L1 and AP3610/3620 Status

L1	Identifi Wireless AP3610/3620 general state
Blink Green	Initialization and discovery in progress via Ethernet
Blink Amber	Initialization and discovery in progress via WDS
Blink Red	Error during initialization and discovery
Solid Green	Discovery finished via Ethernet
Solid Amber	Discovery finished via WDS

LEDs L3 and L4

LEDs L3 and L4 indicate the detailed state of the AP. LEDs L1, L3, and L4 work in conjunction to indicate the general and detailed state of the AP.

[Table 31: LEDs L3, L4 and L1, and AP3610/3620 Detailed State](#) on page 197 provides a composite view of the three LEDs and the corresponding state of the AP:

Table 31: LEDs L3, L4 and L1, and AP3610/3620 Detailed State

L3	L4	L1	Identifi Wireless AP3610/3620 detailed state	
Off	Off	Blink Green	Initialization: Power-on self test (POST)	
		Blink Green		
		Blink Red		
	Solid Green	Blink Green		
		Blink Red		
		Blink Amber		
Blink Green	Off	Blink Green / Orange	Network discovery: 802.1x authentication	
		Blink Red	Failed 802.1x authentication	
	Blink Green	Blink Green / Amber	Network discovery: DHCP	
		Blink Red	Default IP address	
	Solid Green	Blink Green / Amber	Blink Green / Amber	Network discovery: EWC discovery / connect
			Blink Red	Discovery failed
Solid Green	Off	Blink Green / Amber	Connecting to EWC: Registration	
		Blink Red	Registration failed	
	Blink Green	Blink Green / Amber	Connecting to EWC: Image upgrade	
		Solid Green / Amber	AP operating normally: Forced image upgrade	
	Blink Red		Image upgrade failed	

Table 31: LEDs L3, L4 and L1, and AP3610/3620 Detailed State (continued)

L3	L4	L1	IdentifiFi Wireless AP3610/3620 detailed state
	Solid Green	Blink Green / Amber	Connecting to EWC: Configuration
		Blink Red	Configuration failed

After initialization and discovery is completed and the AP3610/3620 is connected to the IdentifiFi Wireless Controller, the LEDs L3 and L4 indicate the state of the corresponding radio – L3 for Radio 5 GHz, and L4 for Radio 2.4 GHz.

[Table 32: LEDs L3 and L4, and Corresponding Radio State](#) on page 198 provides a view of the LEDs L3 and L4 and the corresponding radio state after the discovery is completed.

Table 32: LEDs L3 and L4, and Corresponding Radio State

L3/L4	Radio status
Off	Radio off
Solid Blue	Radio in HT mode
Solid Green	Radio in legacy mode

LED L2

The LED L2 indicates the status of the Ethernet port:

Table 33: LED L2 and Ethernet Port's Status

L2	Ethernet port's status
Off	No Ethernet connection: WDS is enabled
Solid Blue	1 Gb Ethernet connection
Solid Green	100 Mb Ethernet connection
Solid Amber	10 Mb Ethernet connection

**Note**

A 10 Mb Ethernet connection is considered a warning state since it is not sufficient to sustain a single radio in the legacy 11g or 11a modes.

LEDs Indicating WDS Strength for AP3610 and AP3620

The AP indicates the WDS signal strength as a bar graph. To avoid confusion with startup LED behavior, the patterns go from right to left and an LED is always blinking at least twice as fast as the LEDs in normal mode.

[Table 34: AP3610 and AP3620 LEDs Indicating Signal Strength](#) on page 199 illustrates the LED behavior in WDS Signal Strength mode for AP models AP3610 and AP3620.

Table 34: AP3610 and AP3620 LEDs Indicating Signal Strength

RSS (dBm)	LED			
	L1	L2	L3	L4
RSS < -84	Off	Off	Off	Blinking green
-84 < RSS < -77	Off	Off	Off	Fast Blinking green
-77 < RSS < -70	Off	Off	Blinking green	Solid green
-70 < RSS < -63	Off	Blinking green	Solid green	Solid green
-63 < RSS < -56	Blinking green	Solid green	Solid green	Solid green
RSS < -56	Fast Blinking green	Solid green	Solid green	Solid green

**Note**

The LEDs on the AP3605 do not indicate WDS signal strength.

26xx and Other Legacy Wireless APs

Legacy Extreme Networks Wireless APs are the first generation access points marketed by Extreme Networks. Many are still in service worldwide and are still supported by Extreme Networks. They are 80211a/b/g compliant, with the a, b, and g protocols. The LED indicators on these are described in the following subsections:

- [IdentifiFi Wireless AP2610, AP2620 LED Status](#) on page 199
- [IdentifiFi Wireless Outdoor AP2650, AP2660 Wireless AP LED Status](#) on page 203
- [AP4102 and AP2605 LED Status](#) on page 205

IdentifiFi Wireless AP2610, AP2620 LED Status

The following figure depicts the location of the three LEDs on the IdentifiFi Wireless AP2610 and AP2620 models.

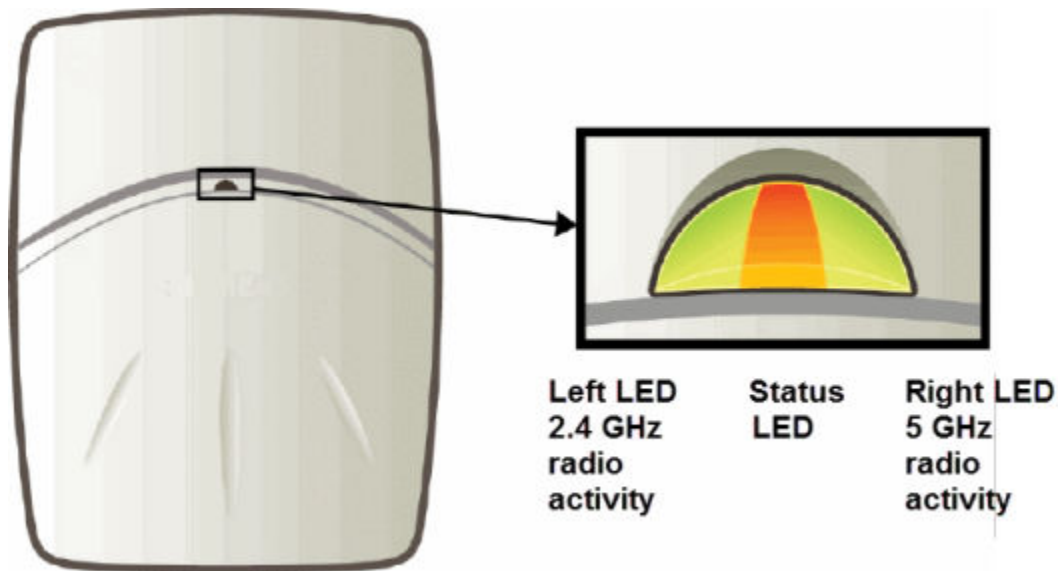


Figure 22: IdentifiFi Wireless AP2610/2620 LEDs

LED Color Codes

The AP2610/2620 LEDs indicate “normal-operation”, “warning/special”, or “failed” state of the AP in the following color codes:

- Green — Indicates the normal-operation state.
- Orange/Amber — Indicates the warning, or special state such as WDS.
- Red — Indicates the error state.
- Blinking — Indicates that the state, such as initialization, or discovery is in progress.
- Steady — Indicates that the state is stable/completed. For example, initialization finished, or discovery completed.

Center LED

The Center LED indicates the general status of the AP2610/2620:

Table 35: Center LED and AP2610/2620 Status

Center LED	IdentifiFi Wireless AP2610/2620 status
Blinking Green	Initialization and discovery in progress via Ethernet link
Blinking Orange/Amber	Initialization and discovery in progress via WDS link
Blinking Red	Error during initialization/discovery process
Solid Red	Irrecoverable error
Solid Green	Discovery finished via Ethernet link
Solid Orange/Amber	Discovery finished via WDS link

Left LED

The Left LED indicates the high-level state of the AP2610/2620 during the initialization and discovery process:

Table 36: Left LED and AP2610/2620 High-level State

Left LED	Identifi Wireless AP2610/2620 high-level state
Off	Initialization
Blinking Green	Network Discovery
Solid Green	Connecting with the Identifi Wireless Controller

Left and Right LEDs

The Right LED indicates the detailed state during the initialization and discovery processes:

Table 37: Left and Right LEDs and AP2610/2620 Detailed State

Left LED	Right LED	Identifi Wireless AP2610/2620 detailed state
Off	Off	Initialization: Power-on self-test (POST)
	Blinking Green	Initialization: Random delay
	Solid Green	Initialization: Vulnerable period
Blinking Green	Off	Network Discovery: 802.1x authentication
	Blinking Green	Network Discovery: Attempting to obtain IP address via DHCP
	Solid Green	Network Discovery: Discovered Identifi Wireless Controller
Solid Green	Off	Connecting to Identifi Wireless Controller: Attempting to register with the Identifi Wireless Controller
	Blinking Green	Connecting to Identifi Wireless Controller: Upgrading to higher version
	Solid Green	Connecting to Identifi Wireless Controller: Configuring itself

Composite View of the Three LEDs

The Center, Left and the Right LEDs work in conjunction to indicate the general, high-level state and the detailed state respectively.

[Table 38: Composite View of Three LED Lights](#) on page 201 provides a composite view of the three LED lights of the AP2610/2620 state:

Table 38: Composite View of Three LED Lights

Left LED	Right LED	Center LED	Identifi Wireless AP's Detailed state
Off	Off	Blinking Green	Initialization: Power-on self-test (POST)
		Blinking Green	Initialization: Random delay
		Blinking Red	Initialization: Neither Ethernet nor WDS link
	Solid Green	Blinking Green	Initialization: Vulnerable period
		Blinking Red	Reset to factory defaults
		Blinking Orange	WDS scanning
Blinking Green	Off	Blinking Green/ Orange	Network discovery: 802.1x authentication

Table 38: Composite View of Three LED Lights (continued)

Left LED	Right LED	Center LED	IdentifiFi Wireless AP's Detailed state
		Blinking Red	Failed 802.1x authentication
	Blinking Green	Blinking Green/ Orange	Network discovery: DHCP
		Blinking Red	Default IP address
	Solid Green	Blinking Green/ Orange	Network discovery: EWC discovery / connect
		Blinking Red	Discovery failed
Solid Green	Off	Blinking Green/ Orange	Connecting with IdentifiFi Wireless Controller: Registration
		Blinking Red	Registration failed
	Blinking Green	Blinking Green/ Orange	Connecting with IdentifiFi Wireless Controller: Image upgrade
		Solid Green/ Orange	AP operating normally: Forced image upgrade
		Blinking Red	Image upgrade failed
	Solid Green	Blinking Green/ Orange	Connecting with IdentifiFi Wireless Controller: Configuration
Blinking Red		Configuration failed	

**Note**

The Left and Right LEDs turn on after the Center LED. This allows you to distinguish easily between the Center LED and the Left/Right LEDs.

**Note**

If the Center LED begins blinking RED, it indicates that the AP's state has failed.

**Note**

Random delays do not occur during normal reboot. A random delay only occurs after a vulnerable period power-down. The AP can be reset to its factory default settings. For more information, see the Extreme Networks IdentifiFi Wireless Maintenance Guide.

LEDs Indicating WDS Strength for AP2610 and AP2620

The AP indicates the WDS signal strength as a bar graph. To avoid confusion with startup LED behavior, the patterns go from right to left and an LED is always blinking at least twice as fast as the LEDs in normal mode.

[Table 39: AP2610 and AP2620 LEDs Indicating Signal Strength](#) on page 203 illustrates the behavior of the three LED lights of the AP's WDS strength.

Table 39: AP2610 and AP2620 LEDs Indicating Signal Strength

RSS (dBm)	Left LED	Middle LED	Right LED
RSS < -84	Off	Off	Blinking green
-84 < RSS < -77	Off	Off	Fast Blinking green
-77 < RSS < -70	Off	Blinking green	Solid green
-70 < RSS < -63	Blinking green	Solid green	Solid green
RSS < -63	Fast Blinking green	Solid green	Solid green

IdentifiFi Wireless Outdoor AP2650, AP2660 Wireless AP LED Status

All AP models have the LEDs L1, PoE, P1, R1, R2 and F which are used to indicate the status of the AP. For the position of the LEDs, refer to the respective AP manual.

The following figure depicts the location of the LEDs on the IdentifiFi Wireless Outdoor AP2660.

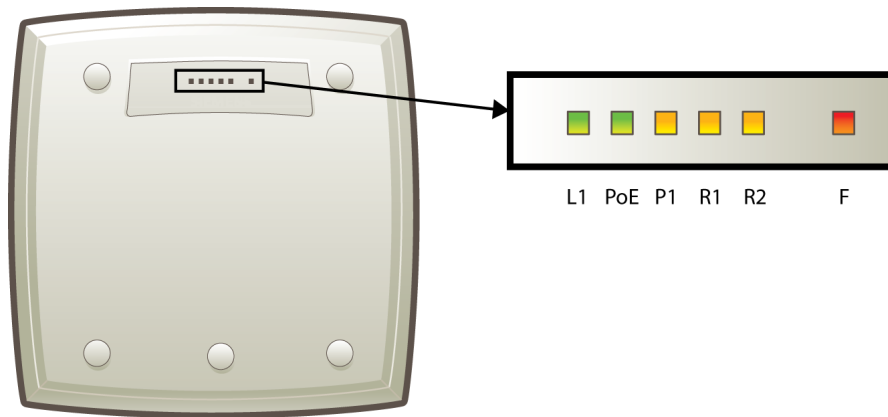


Figure 23: IdentifiFi Wireless Outdoor AP2660 LEDs

The R1, R2 and F LEDs work in conjunction to indicate the general, high-level and detailed state respectively. The remaining LEDs indicate link status.

Table 40: [IdentifiFi Wireless Outdoor AP2660 LED Status](#) on page 203 provides a composite view of the R1, R2 and F LEDs:

Table 40: IdentifiFi Wireless Outdoor AP2660 LED Status

R1 LED	R2 LED	F LED	IdentifiFi Wireless Outdoor AP2660 detailed status
Off	Off	Blinking Red	Initialization: Power-on-self test (POST)
	Blinking Green	Blinking Red	Initialization: Random delay
	Solid Green	Blinking Red	Initialization: Vulnerable Period
		Solid Red	Reset to factory defaults
	Solid Green	Blinking Red	WDS scanning
Blinking Green/ Yellow	Off	Blinking Red	Network discovery: 802.1x authentication

Table 40: IdentifiFi Wireless Outdoor AP2660 LED Status (continued)

R1 LED	R2 LED	F LED	IdentifiFi Wireless Outdoor AP2660 detailed status
		Solid Red	Failed 802.1x authentication
	Blinking Green/ Yellow	Blinking Red	Network discovery: DHCP
		Solid Red	Default IP address
	Solid Green/ Yellow	Blinking Red	Network discovery: EWC discovery/connect
		Solid Red	Discovery failed
Solid Green	Off	Blinking Red	Connecting with EWC: Registration
		Solid Red	Registration failed
	Blinking Green/ Yellow	Blinking Red	Connecting with EWC: Image upgrade
		Solid Red	Image upgrade failed
	Solid Green/ Yellow	Blinking Red	Connecting with EWC: Configuration
		Solid Red	Configuration failed
	Blinking Green/ Yellow	Off	AP operating and running normally: Forced image upgrade
		Solid Red	Image upgrade failed

**Note**

After discovery is finished, the R1 and R2 LEDs will be Green for Ethernet uplink, and Yellow for WDS uplink.

**Note**

If a fatal AP error occurs, the F LED will be solid Red.

LEDS Indicating WDS Strength for AP2650 and AP2660

The AP indicates the WDS signal strength as a bar graph. To avoid confusion with startup LED behavior, the patterns go from right to left and an LED is always blinking at least twice as fast as the LEDs in normal mode.

[Table 41: AP2650 and AP2660 LEDs Indicating Signal Strength](#) on page 204 illustrates the behavior of the LED in WDS Signal Strength for AP models AP2650 and AP2660.

Table 41: AP2650 and AP2660 LEDs Indicating Signal Strength

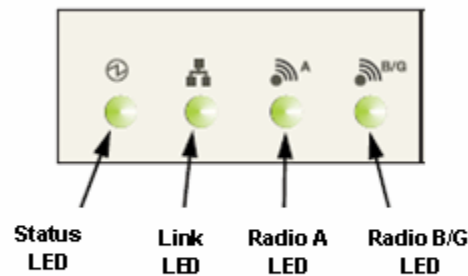
RSS (dBm)	LED					
	L1	PoE	P1	R1	R2	F
RSS < -84	Off	Off	Off	Off	Off	Blinking red
-84 < RSS < -77	Off	Off	Off	Off	Off	Fast Blinking red
-77 < RSS < -70	Off	Off	Off	Off	Blinking green	Solid red
-70 < RSS < -63	Off	Off	Off	Blinking green	Solid green	Solid red

Table 41: AP2650 and AP2660 LEDs Indicating Signal Strength (continued)

RSS (dBm)	LED					
	L1	PoE	P1	R1	R2	F
-63 < RSS < -56	Off	Off	Blinking green	Solid green	Solid green	Solid red
-56 < RSS < -49	Off	Blinking green	Solid green	Solid green	Solid green	Solid red
-49 < RSS < -42	Blinking green	Solid green	Solid green	Solid green	Solid green	Solid red
RSS < -42	Fast Blinking green	Solid green	Solid green	Solid green	Solid green	Solid red

AP4102 and AP2605 LED Status

The following figure shows the LEDs on the AP4102 and AP2605 Access Points.

**Status LED**

The Status LED indicates the general status of the access point.

Table 42: AP4102 and AP2605 Status Indicators

Status LED	AP Status
Blink green	Initialization and discovery in progress via Ethernet or WDS link
Blink amber	Error during initialization and discovery
Solid green	Discovery finished via Ethernet or WDS link

Radio B/G LED

The Radio B/G LED will show the general high-level state during initialization and discovery for the access point.

Table 43: AP4102 and AP2605 Initialization and Discovery Indicators

Radio B/G LED	AP High-Level State
Off	Initialization
Blink green	Network discovery
Solid green	Connecting with IdentifiFi Wireless Appliance

Composite View of LEDs

The following table summarizes all LEDs during the initialization and discovery.

These states will be shown together with a status LED blinking green or orange. If the status LED is blinking green, the state will be the one executed by the AP in that moment. If the status LED is blinking orange, the state will be the one that the AP failed.

The status and radio LEDs will blink with 1/3 pulse width, but the radio LEDs will turn on after the status LED. This solution also allows the user to distinguish easily between the status LED and the radio LEDs.

Table 44: AP4102 and AP2605 Composite View of LEDs

Radio B/GLED	Radio A LED	Status LED	AP Detailed State
Off	Off	Blink green	Initialization: Power-on self test (POST)
	Blink green	Blink green	Initialization: Random delay
		Blink orange	Initialization: No Ethernet nor WDS link
	Solid green	Blink green	Initialization: Vulnerable period
		Blink orange	Reset to factory defaults
	Solid green	Blink green	WDS scanning
Blink green	Off	Blink green	Network discovery: 802.1x authentication
		Blink orange	Failed 802.1x authentication
	Blink green	Blink green	Network discovery: DHCP
		Blink orange	Default IP address
	Solid green	Blink green	Network discovery: EWC discovery / connect
		Blink orange	Discovery failed
Solid Green	Off	Blink green	Connecting with EWC: Registration
		Blink orange	Registration failed
	Blink green	Blink green	Connecting with EWC: Image upgrade
		Blink orange	Image upgrade failed
	Solid green	Blink green	Connecting with EWC: Configuration
		Blink orange	Configuration failed
	Blink green	Solid green	AP up and running: Forced image upgrade
		Blink orange	Image upgrade failed

LEDs Indicating WDS Strength for AP4102 and AP2605

The AP indicates the WDS signal strength as a bar graph. To avoid confusion with startup LED behavior, the patterns go from right to left and an LED is always blinking at least twice as fast as the LEDs in normal mode.

[Table 45: AP4102 and AP2605 LEDs Indicating Signal Strength](#) on page 207 illustrates the LED behavior in WDS Signal Strength mode for AP models AP4102 and AP2605.

Table 45: AP4102 and AP2605 LEDs Indicating Signal Strength

RSS (dBm)	LED			
	Status	Link	Radio A	Radio B/G
RSS < -84	Off	Eth state	Off	Blinking green
-84 < RSS < -77	Off	Eth state	Off	Fast Blinking green
-77 < RSS < -70	Off	Eth state	Blinking green	Solid green
-70 < RSS < -63	Blinking green	Eth state	Solid green	Solid green
RSS < -63	Fast Blinking green	Eth state	Solid green	Solid green

Configuring Wireless AP LED Behavior

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

Table 46: 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.
WDS Signal Strength	Indicates the WDS signal strength as a bar graph. See Table 39: AP2610 and AP2620 LEDs Indicating Signal Strength on page 203, Table 41: AP2650 and AP2660 LEDs Indicating Signal Strength on page 204, Table 34: AP3610 and AP3620 LEDs Indicating Signal Strength on page 199, and Table 45: AP4102 and AP2605 LEDs Indicating Signal Strength on page 207 for a description of LED behavior. This setting helps to align external antennas in WDS deployments by correlating the WDS link RSS with the LED pattern. Use this setting only if the AP operates in WDS mode by being a member of a WDS VNS.

You can configure the AP LED mode when you configure:

- 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.

To Configure the AP LED Operational Mode When Configuring an Individual Wireless AP:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left-hand pane, click **APs**, then **All**. The **AP Configuration** page displays with the **AP Properties** tab exposed.
- 3 In the second column from the left, select the appropriate AP.
- 4 On the **AP Properties** tab, click the **Advanced** button. The **Advanced** window displays.
- 5 In the **LED** field, click the arrow and select an LED operational mode. See [Table 46: LED Operational Modes](#) on page 207 for a description of each option.

To Set the AP LED Operational Mode When Using the AP Multit-edit Feature:

- 6 From the top menu, click **AP**. The **AP** screen displays.
- 7 In the left-hand pane, click **Bulk Configuration**, then **AP Multi-edit**. The **AP Multi-edit** window displays.
- 8 In the **Wireless AP** section, select one or more **APs**. The **AP Configuration** screen displays.
- 9 In the **AP Configuration** section, locate the LED field. Click the arrow and select an LED operational mode. See [Table 46: LED Operational Modes](#) on page 207 for a description of each option.

To Set the AP LED Operational Mode When Configuring Default AP Behavior:

- 10 From the top menu, click **AP**. The **AP** screen displays.
- 11 In the left pane, click **Bulk Configuration**, then **AP Default Settings**. The **AP Default Settings** page displays with the **Common Configuration** tab exposed.
- 12 Click the AP tab that corresponds to the type of AP that you want to configure. The **AP Properties** and **Radio** settings become available.
- 13 Click the **Advanced** button. The **Advanced** window displays.

In the LED field, click the arrow and select an LED operational mode. See [Table 46: LED Operational Modes](#) on page 207 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
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.

Extreme Networks IdentiFi Wireless 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.

On the **Topologies** configuration page, a number of parameters related to network topology can be defined:

- VLAN ID and associated L2 port
- L3 (IP) interface presence and the associated IP address and subnet range
- The rules for using DHCP
- 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 210.

Configuring the Admin Port

The Admin port is a physical ethernet port directly connected to the controller's management plane. As its name suggests, it is intended to provide a dedicated connection to a secure management VLAN. The controller can use the Admin port to interact with RADIUS, SNMP, and NetSight servers.

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

The screenshot shows the 'Topologies' configuration page in the controller's GUI. The left sidebar is expanded to 'Network' > 'Topologies'. The main area displays a table of topologies and their configurations.

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'. At the bottom, there are input fields for 'Internal VLAN ID: 1' and 'Multicast Support: Port1'. A 'Save' button is located at the bottom right of the main content area.

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

- Under Core, the Admin port **Name** and **Mode** are not configurable.
- 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 56).

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 56).
 - 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.

Click Refresh to refresh the list of Dynamic IP Addresses.

- 7 Click **Save** to save your changes.
- 8 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 for configuring topologies. 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 'Topologies' and contains a table with the following data:

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 for 'New', 'New Group', and 'Delete Selected'. There are also configuration fields for 'Internal VLAN ID: 1' and 'Multicast Support: Disabled'. A 'Save' button is located at the bottom right.

- 2 If you want to edit an existing topology, select the desired topology. If you want to create a new topology, click the **New** button. Depending on your selection, two or three tabs are displayed.
- 3 Proceed to [Configuring a Basic Topology](#) on page 213 to create and save the new topology. Optional configuration options are also described.

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 If you want to edit an existing topology, select the desired topology. If you want to create a new topology, click the **New** button. Depending on your selection, two or three tabs are displayed.

The screenshot shows the 'Topology: General' configuration page. The left sidebar has 'Topologies' selected. The main area has two tabs: 'General' and 'Multicast Filters'. Under 'General', there are three sections: 'Core' with 'Name' (text input 'name') and 'Mode' (dropdown 'Bridge Traffic Locally at EWC'); 'Layer 2' with 'VLAN Setting' (VLAN ID: text input, range '1 - 4094', radio buttons for 'Untagged' and 'Tagged', and 'Port' dropdown); and 'Layer 3' with a 'Layer 3' checkbox, 'Layer 3 - IPv4' text input, and 'Mask (optional)' text input. A 'Save' button is at the bottom right.

- 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 217 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 DHCP, 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 Link Aggregation (LAG) data port. For more information, see [Viewing and Changing the L2 Ports Information](#) on page 57.
- 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**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Topologies** . The **Topologies** tab displays.

- 3 Click **New Group**. The **Topology Group** screen displays.

Topology Group:

General

Core

Name:

Mode: Routed

Layer 2

VLAN Setting: VLAN ID: (1 - 4094)

Topologies

Topology Name	VLAN ID	Tagged	Port	IP Address

- 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 member topologies. A topology group must contain at least 1 topology.
- 8 To add/delete a member topology from the topology group, click **Edit** under Topologies. Check/uncheck the left side box to add/remove the member topology.
- 9 To delete a topology group, just select it and click **Delete**. When a topology group is deleted, only the group is deleted, not the topologies it contained.
- 10 To delete a Topology Group, select the topology from the list of Topology Groups, and click **Delete Selected**.
- 11 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 230.

To Enable Management Traffic for a Topology:

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

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

Layer 3 Configuration

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

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 DHCP, 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** and then from the left pane select **Topologies**. Alternatively, from the top menu select **VNS > Topologies**.
- 2 If already defined, click the topology you want to define the IP address for. The **Topologies** window is displayed. Alternatively, press the **New** button to create a new topology. Depending on the preselected options, two or three tabs are displayed.

- 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.

DHCP Configuration

You can configure DHCP 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 Navigate to the Topology page.
- 2 On the Topology page, click the General tab and enable Layer 3.
- 3 From the **DHCP** drop-down list, select one of the following options and click the **Configure** button.
 - **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.
- 4 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.

- 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**. The DHCP Address Exclusion dialog closes.
- 1 The **Broadcast Address** box populates automatically based on the Gateway IP address and subnet mask of the VNS.
 - 2 Click Close.
- 5 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 controllers'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.

- 6 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**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the **Topologies** pane, then click the routed Topology you want to define a next-hop route for.
- 3 In the Layer 3 area, click the **Configure** button. The DHCP configuration dialog window displays.

- 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 To save your changes, 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 un-rolling 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 prepended 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.

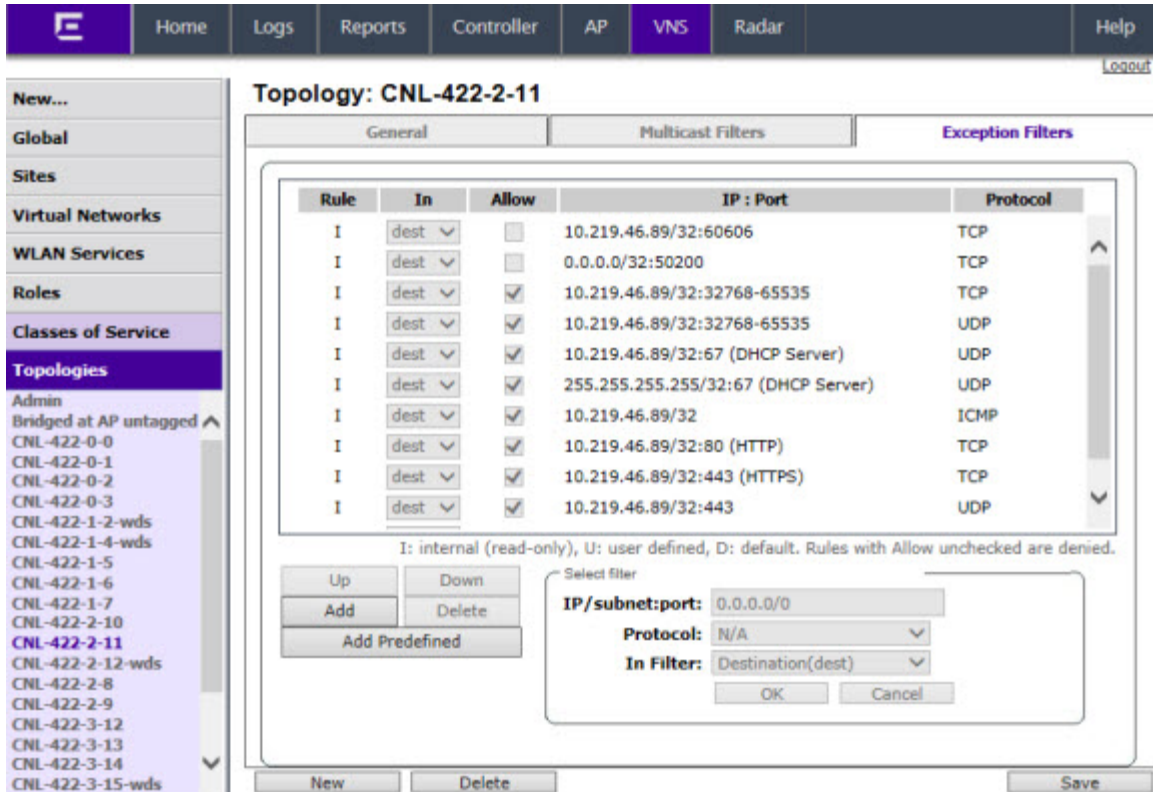
The exception rules are evaluated in the context of referring to the specific controller's interface. The destination address for the role rule definition is typically defined as the interface's own IP address. The port number for the filter definition corresponds to the target (destination) port number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



- 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 47: 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.

Table 47: Exception Filters page - Fields and Buttons (continued)

Field/Button	Description
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	<p>Advanced filtering mode provides the ability to create bidirectional filters.</p> <p>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.</p> <p>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.</p>
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.
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 56.

To Enable Multicast for a Topology:

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

The screenshot shows the 'Topology: Bridged at AP untagged' configuration page. The 'Multicast Filters' tab is active. A checkbox for 'Multicast bridging' is checked, with a note that only matching rules will be allowed. Below this is a table with columns for IP, Group, and Wireless Replication. One rule is defined: IP '0.0.0.0/0', Group 'All Multicast', and Wireless Replication checked. Below the table are radio buttons for 'IP Group' (unselected) and 'Defined groups' (selected), with a dropdown menu showing 'All Multicast (0.0.0.0/0)'. There are 'Up', 'Down', 'Add', and 'Delete' buttons. At the bottom are 'New', 'Delete', and 'Save' buttons.

IP	Group	Wireless Replication
0.0.0.0/0	All Multicast	<input checked="" type="checkbox"/>

- 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.
- 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 2 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 305 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 Roles](#) on page 228.

In general, Class of Service (CoS) refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a 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**.
The **Virtual Network Configuration** screen displays.
- 2 In the left pane expand the **Roles** pane and click the role you want to edit, or click the **New** button to create a new role.

The Role configuration page displays. By default, the **VLAN & Class of Service** tab displays the following figure.

The screenshot shows the 'Role: VLAN & Class of Service' configuration page. The left sidebar has a menu with 'Roles' highlighted. The main content area has two tabs: 'VLAN & Class of Service' (active) and 'Policy Rules'. Under the 'Core' section, there is a 'Role Name' text input field. Under the 'Default Action' section, there are three dropdown menus: 'Access Control' (set to 'None'), 'Default Class of Service' (set to 'No change'), and 'Traffic Mirror' (set to 'None'). To the right of these dropdowns are 'Edit' and 'New' buttons. At the bottom right of the configuration area are 'Advanced...' and 'Save' buttons.

Figure 24: VLAN & Class of Service Tab

Table 48: 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	Select from one of the following: <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 - A topology to use when a VNS is created using a role that does not specify a topology.

Table 48: VLAN & Class of Service Tab - Fields and Buttons (continued)

Field/Button	Description
VLAN	<p>Select an existing Topology, Topology Group, or click the New button to create a new Topology.</p> <p>To edit an existing Topology, select the VLAN and then click the Edit button. The Edit Topology page displays. For information about how to configure a Topology, go to Configuring Roles on page 228.</p> <p>Note: VLAN is only visible when the user selects "Contain to VLAN" as the default access control action.</p>
Default Class of Service	<p>Select an existing class of service from the Default Class of Service drop-down list, or click the New button to create a new topology.</p> <p>To edit an existing class of service, select the class of service and then click the Edit button. The Edit Class of Service page displays. For information about how to configure a Class of Service, go to Configuring Roles on page 228.</p>
Traffic Mirror	<p>The port on the controller that receives the traffic mirror (originated in a monitored port). The mirroring port is directly connected to the Purview Engine and can't be used for any other traffic forwarding. The mirroring port can be only L2 port on the controller, not wired interface on the AP or WLAN port. Select from one of the following:</p> <ul style="list-style-type: none"> • None - No role defined • Enable - Default setting • Prohibited - Traffic Mirroring is prohibited for this Role.
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, go to [Working with Bandwidth Control Profiles](#) on page 304 for more information.

Policy Rules

Optionally, you can define policy rules for the 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. However, if you require user-specific filter definitions, then the filter ID configuration identified the specific role that should be applied to the user.

Matching Policy Rules Criteria

The following rules 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 Source IP address
- IPv4 Destination IP address
- Source layer 4 port
- Destination layer 4 port
- IPv4 Source socket (IP address + port)
- IPv4 Destination socket (IP address + port)
- IP type
- ICMP packet type and code
- ToS/DSCP marking
- 802.1p priority
- Ethertype

Policy rule access control actions can be:

- Allow, meaning forward matching frames on the WLAN Service's default topology
- Deny, meaning drop matching frames
- Contain to VLAN, meaning forward matching frames on the indicated VLAN
- None, meaning the rule does not have an access control action. The matching engines essentially ignores a rule with an access control action of 'None'.

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 DHCP 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 it is recommended that the default action of a non-authenticated role be to drop all traffic not matching a rule.

Defining non-authenticated roles allows administrators to identify destinations to which a mobile user is allowed to access without incurring an authentication redirection. Typically, the recommended default rule is to deny all. Administrators should define a rule set that will permit 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 will be 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 will provide a specific IP definition of a server outside the wireless .

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 will be redirected to the allowed destinations. Most HTTP traffic outside of that defined in the non-authenticated filter will be redirected.

Note



Although non-authenticated roles 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 will be discarded by the controller.

The non-authenticated filter is applied by the controller 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

A basic non-authenticated role for internal Captive Portal should have three rules, in the following order:

Table 49: 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

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

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

Table 50: 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 will 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

Below are two examples of possible policy rules for authenticated users. The first example disallows some specific access before allowing everything else.

Table 51: Policy Rules Example A

In	Out	Allow	IP / Port	Description
x	x		*.*.*.*:22-23	SSH and telnet 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 second example does the opposite of the first example. It allows some specific access and denies everything else.

Table 52: 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 will apply only after:

- 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 will ensure that a packet is not dropped entirely if no other match can be 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 53: Default Role Example A

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

Table 54: Default Role Example B

In	Out	Allow	IP / Port	Description
	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 telnet (port 23) or FTP (port 21)
	x	x	10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network
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 are connected to the same AP will pass through the controller and therefore be subject to 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 ID filter, before allowing everything else:

Table 55: 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 244.

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. Different AP models support different numbers of policy rules per role. Most AP2600 models accept a maximum of 32 rules per role. The 3600 and 3700 series APs accept a maximum of 64 rules per role. 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 can use more than one type of topology. If a role uses at least one Bridged at AP topology the AP will filter all inbound traffic assigned to the rule. The controller will perform all outbound filtering.

Wireless AP Filtering

When filtering at the wireless AP is enabled, APs obtain client filter information from the controller. In addition, direct inter-AP communication allows APs to exchange client filter information as clients roam from one AP to another. This allows the system to achieve a very fast roaming time. To take advantage of inter-AP communication, you should configure the network such that APs in the mobility domain can communicate with each other through the AP's Ethernet interface. Also, multicast traffic with an IP address of 224.0.1.178 should be allowed between APs.

Configuring Policy Rules

To Configure Policy Rules:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 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 **Role configuration** page is displayed.
- 3 Click the **Policy Rules** tab.
The **Rules** tab displays. See [Figure 25: Policy Rules Page - Rules Tab](#) on page 237.
- 4 To add a new rule, click **Add**. The **Filter Rule Definition** dialog appears (see [Figure 27: Filter Rule Definition Dialog](#) on page 240). For more information on the dialog, see [Table 57: Filter Rule Definition Dialog - Fields and Buttons](#) on page 240.
- 5 To edit a rule, click on its row in the table, then click **Edit**.
- 6 To delete a rule click on its row in the table, then click **Delete**.

Custom AP Filters:

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. To allow the AP to 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 with older AP 2600 series APs.

There are a number of restrictions on a role that uses custom AP filtering including:

- Cannot use Layer 2 filter rules
- 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.

To create a custom AP Filter:

- 1 Select the **AP Filtering** checkbox to enable the policy rules defined on the **Rules** tab to be applied by APs. The Custom AP Rules checkbox becomes available.
- 2 Select the **Custom AP Rules** checkbox to configure additional rules for the APs. A **Custom AP Rules** tab is added to the window.
- 3 Click the **Custom AP rules** tab. See [Figure 26: Policy Rules Page - Custom AP Rules Tab](#) on page 238.
- 4 Configure policy rules for the APs.

Role: CNL-422-0-1-default

VLAN & Class of Service | Policy Rules

Inherit filter rules from currently applied role ⓘ

Rules AP Filtering Custom AP Rules

In	Out	EthType	MAC	IP : Port	Protocol	Priority	ToS/DSCP	Access
dest	src	0x0800	Any	0.0.0.0/0:67 (DHCP S	UDP	Any	N/A	Allow
dest	none	0x0800	Any	0.0.0.0/0	Any	Any	N/A	Allow
none	src	0x0800	Any	0.0.0.0/0	Any	Any	N/A	Allow

Add Edit Delete Up Down Top Bottom

New Delete Save

Figure 25: Policy Rules Page - Rules Tab

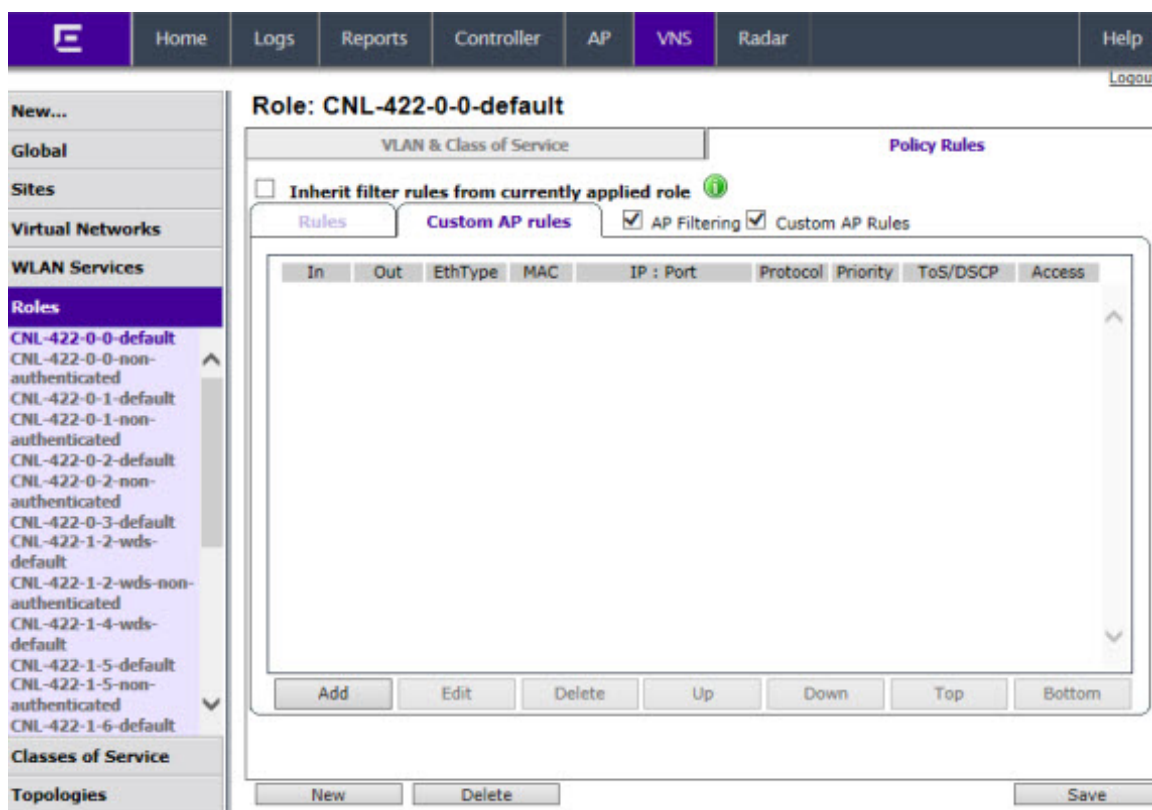


Figure 26: Policy Rules Page - Custom AP Rules Tab

Table 56: 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	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. 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”.
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	

Table 56: Policy Rules Tab - Fields and Buttons (continued)

Field/Button	Description
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 307.</p>
Ethtype	Displays the Ethertype filter for the selected policy rule.
MAC	Displays the destination MAC address for the selected layer 2 policy rule.
IP:Port	Displays the IP address and port to which this policy rule applies.
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
Priority	Identifies an 802.1p priority to match. Can be "Any" meaning that it is not actually part of the match. From the drop-down menu select from Priority 0 to Priority 7.
ToS/DSCP	Identifies the Type of Service (ToS) and Diffserv Codepoint (DSCP) classification to match. Can be "Any".
Access	Identifies the access control protocol to match.
Add	Click to add a new rule. The Policy Rule Definition dialog displays. See Figure 27: Filter Rule Definition Dialog on page 240.
Edit	Click to edit the selected definition.
Delete	Click to remove this role rule.
Up, Down	Select a role rule and click to either move the rule up or down in the list. The policy rules are executed in the order in which you define them.
Save	Click to save the configuration.

Figure 27: Filter Rule Definition Dialog

Table 57: Filter Rule Definition Dialog - Fields and Buttons

Field/Button	Description
Direction	
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 307.</p>
Classification - Layer 2, 3, 4	
Ethertype	Select a matching Ethertype filter for the selected policy rule.

Table 57: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Mac Address	Select a MAC Address from the drop-down list.
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 role 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: 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 383.
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	Select from one of the following pre-defined IDs to support L5+ filtering: <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	Select from one of the following: <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.

Table 57: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Class of Service	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 228.
Traffic Mirror	Select from one of the following: <ul style="list-style-type: none">• None - No rule defined• Enable - Default setting• Prohibited - Traffic Mirroring prohibited for this Filter Rule.
OK	Click to add the role rule to the filter group. The information is displayed in the role rule table.
Cancel	Click Cancel to discard your changes.

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

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 IdentifiFi Wireless 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 454.

A third-party AP WLAN Service allows for the specification of a segregated subnet by which non-Extreme Networks IdentifiFi Wireless 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 From the top menu, click **VNS**. Then, in the left pane, select **WLAN Services**.

The WLAN Services window displays.

- 2 To create a new service, click the **New** button. The New WLAN Services configuration window displays.

The screenshot shows a web interface for configuring WLAN services. At the top, there is a navigation bar with tabs: Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A 'Logout' link is visible in the top right corner. On the left side, there is a sidebar menu with categories: New..., Global, Sites, Virtual Networks, WLAN Services (highlighted), Roles, Classes of Service, and Topologies. 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 contains a 'WLAN Services' configuration box. This box has a 'Name:' text input field, a 'Service Type:' section with radio buttons for Standard (selected), WDS, Mesh, Third Party AP, and Remote, and an 'SSID:' text input field. Below this is a 'Status' section with an 'Enable:' checkbox that is checked. A 'Save' button is located at the bottom right of the configuration area.

- a Enter a name for the WLAN service.
- b Select the service type.
- c Change the SSID (optional).
- d Click **Save**.

The **WLAN Services Configuration** page displays.

- To edit an existing service, select the desired service from the left pane. The **WLAN Services Configuration** page displays. [Table 58: WLAN Services Configuration Page](#) on page 246 describes the WLAN services configuration page fields and buttons.

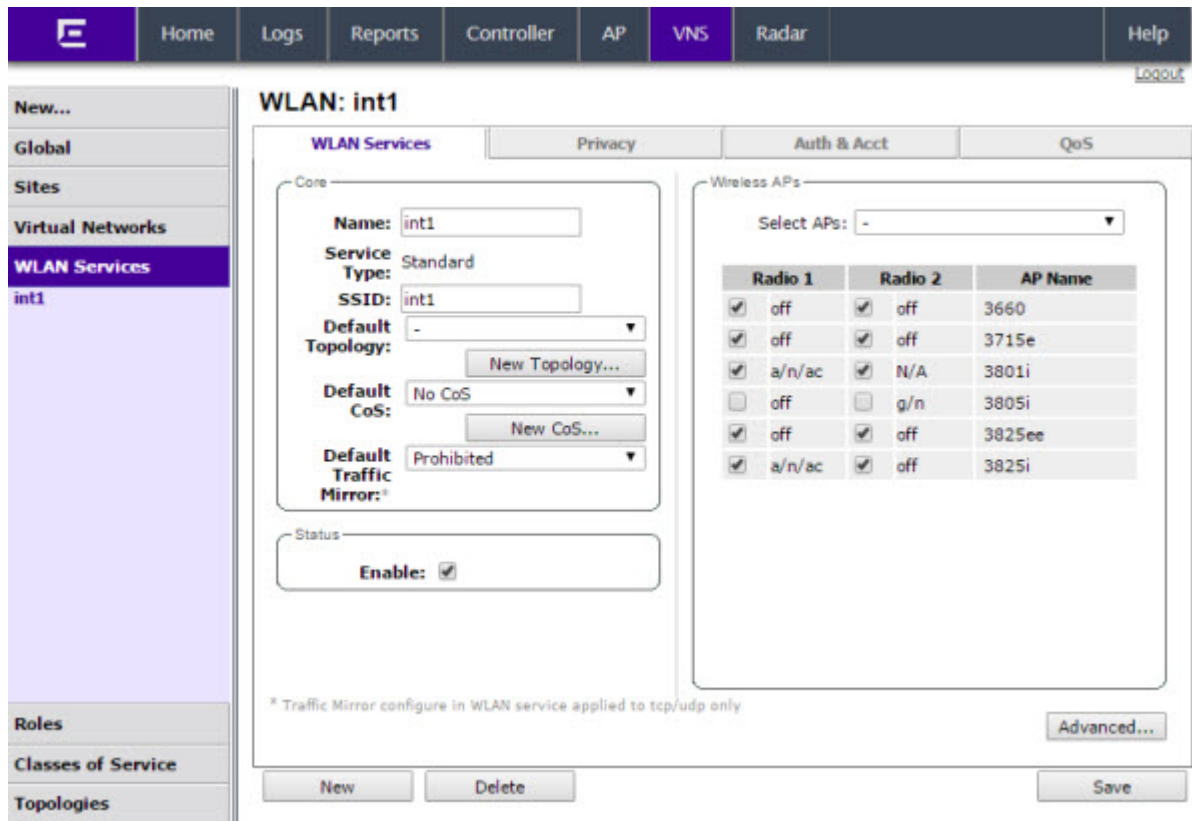


Table 58: WLAN Services Configuration Page

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 58: 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 212 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 CoS	<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 379 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>Select from one of the following:</p> <ul style="list-style-type: none"> • Prohibited - No traffic flow defined. • Enable both directions - Enables traffic flow for both ingress (input interface) and egress (output intrerface). • Enable in direction only - Enables traffic flow in a single direction. Ingress (input interface) and egress (output intrerface). <p>Note: Traffic Mirror configured in WLAN service applies to TCP/UDP only.</p>
Status	
Enable	<p>Select the checkbox to enable this WLAN service. Otherwise, deselect this checkbox. The WLAN service is enabled by default, unless the number of supported enabled WLAN Services has been reached.</p>
Wireless APs	

Table 58: WLAN Services Configuration Page (continued)

Field/Button	Description
Select APs	<p>Select APs and their radios by grouping. Options include:</p> <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 430), 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.
Advanced	Click to access the WLAN service advanced configuration options. The Advanced configuration page options are described in Table 59: Advanced WLAN Service Configuration Page on page 248.
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.

Table 59: 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.

Table 59: Advanced WLAN Service Configuration Page (continued)

Field/Button	Description
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. This feature is only applicable to 37xx and 38xx APs using Build V9.21 or later AP images.
Egress Filtering Mode	
Enforce explicitly defined "Out" rules	Traffic is filtered as configured. For more information, see Configuring Egress Filtering Mode on page 307.
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 307.
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	
8021D Base Port: xxx	The 802.1D Base Port number in the 802.1D area is the port number by which NetSight 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	

Table 59: Advanced WLAN Service Configuration Page (continued)

Field/Button	Description
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 associated 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 Role	Select the checkbox to apply the default non-authenticated role to all traffic flowing to and from an unauthenticated station.
Netflow	Click to Enable/Disable Netflow flag.
Close	Click to close this page.

**Note**

If two controllers have been paired for availability (for more information, see [Availability](#) on page 430), each controller's registered wireless APs are displayed as foreign in the list of available APs on the other controller.

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 — Identifi Wireless Appliance, Identifi Wireless Outdoor AP, and Wireless 802.11n AP — to any VNS.

Configuring Privacy

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

There are five 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 to 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 If the WLAN Service configuration page is not already displayed, 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 60: WLAN Services Privacy Tab - Fields and Buttons](#) on page 254 describes the WLAN services privacy tab fields and buttons.

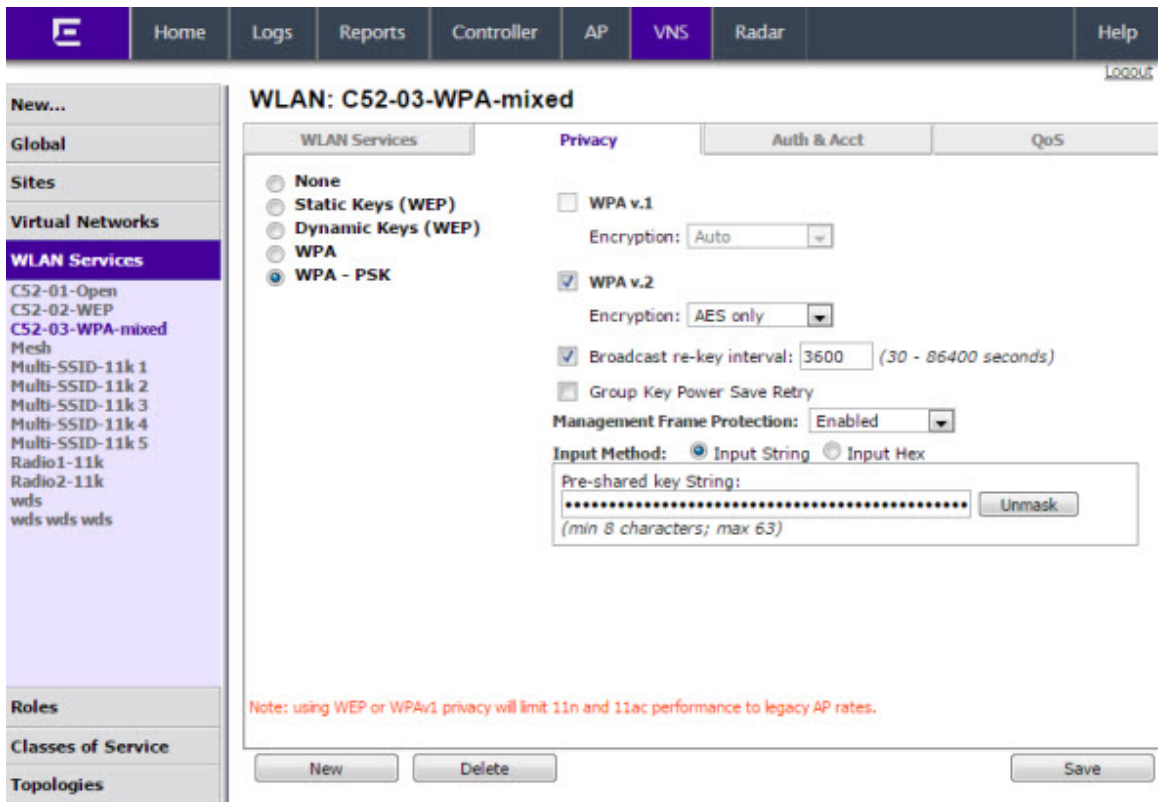


Table 60: WLAN Services Privacy Tab - Fields and Buttons

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. Specifying the WEP key index is supported only for AP36XX APs. 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 60: 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 60: 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 253. • Pre-authentication — Enables seamless roaming. For more information, see Configuring WLAN Service Privacy on page 253. • Opportunistic Keying & Pre-auth — For more information, see Configuring WLAN Service Privacy on page 253.
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>
Group Key Power Save Retry	<p>To enable the group key power save retry The group key power save retry is only supported for AP36XX APs.</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>

Table 60: WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
Input Method	Select one of the following input methods: <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.
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:
 - GuestPortal
 - GuestSplash
- 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

Vendor Specific Attributes

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Extreme Networks IdentifiFi Wireless authentication mechanism provides six VSAs for RADIUS and other authentication mechanisms ([Table 61: Vendor Specific Attributes](#) on page 258).

Table 61: 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.
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 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 538.
- **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**. The **Virtual Network Configuration** screen displays.
- 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**.

WLAN: CNL-422-0-0

WLAN Services | Privacy | **Auth & Acct** | QoS

Authentication This type of authentication requires the user to be on a bridged or controller or routed topology.

Mode:

Enable MAC-based authentication

RADIUS Servers

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

Collect Accounting Information of Wireless Controller

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

MAC-Based Authorization Configuration ? X

Options

MAC-based authorization on roam

Automatically Authenticate Authorized Users

Allow Un-Authorized Users

RADIUS accounting begins after MAC-based authorization completes

RADIUS Server Timeout Role

Table 62: MAC-Based Authorization Configuration Dialog - Fields and Buttons

Field/Button	Description
MAC-based authorization on roam	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 293.

- 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:

Password:

- 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 230. 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**. The **Virtual Network Configuration** screen displays.
- 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.

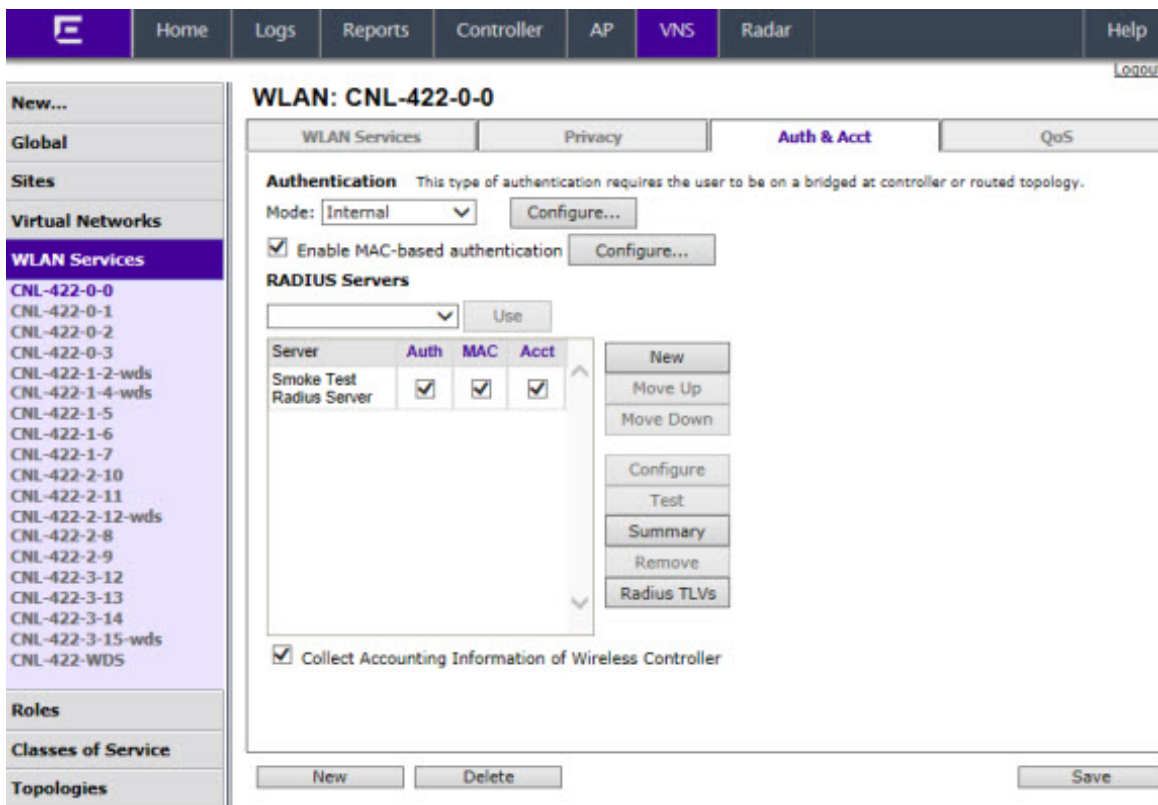


Table 63: WLAN Services Auth & Acct Tab - Fields and Buttons

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 257.
Enable MAC-based authentication	Select to enable the RADIUS server to perform MAC-based authentication for the VNS with Captive Portal.

Table 63: WLAN Services Auth & Acct Tab - Fields and Buttons (continued)

Field/Button	Description
RADIUS Servers	Select the server you want to assign to the WLAN Service from the drop-down list, 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 293. In the Server table, select the checkboxes in the Auth, MAC, or Acct columns, to enable the authentication or accounting, if applicable.
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.

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

RADIUS Access-Request Message Options

VSAs

Include the following Vendor-Specific-Attributes in RADIUS Requests:

Ingress Rate Control VNS Name
 Egress Rate Control AP Name
 Topology Name SSID
 Role Name

Optional TLVs

Include the following Standard-Attributes in RADIUS Requests:

Chargeable-User-Identity
 Treat Access-Accept without Chargeable-User-Identity attribute as Access-Reject

Zone Support

Replace Called Station ID with Zone name in RADIUS Requests

Operator Name: Disabled ▼

OK Cancel

Table 64: 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 266.</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**. The **Virtual Network Configuration** screen displays.
- 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 266
- [Defining RADIUS Settings for Individual RADIUS Servers](#) on page 266
- [Testing RADIUS Server Connections](#) on page 267
- [Viewing the RADIUS Server Configuration Summary](#) on page 268
- [Removing an Assigned RADIUS Server from a WLAN Service](#) on page 269

Defining Common RADIUS Settings

To Define Common RADIUS Settings:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 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:
 - **Ingress Rate Control**
 - **Egress Rate Control**
 - **Topology Name**
 - **Role Name**
 - **VNS Name**
 - **AP Name**
 - **SSID**
 - **Replace Called Station ID with Zone name in RADIUS Requests**

The Vendor Specific Attributes must be defined on the RADIUS server.

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

Defining RADIUS Settings for Individual RADIUS Servers

To Define RADIUS Settings for Individual RADIUS Servers:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 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
?
✕

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: Unmask

OK
Cancel

- 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**. The **Virtual Network Configuration** screen displays.
- 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 **Test RADIUS Servers** screen displays.

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.

- 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**. The **Virtual Network Configuration** screen displays.

- 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.
- In the **Server** table, click a RADIUS server whose configuration summary you want to view, and then click **Summary**. The **RADIUS Summary** screen displays.

The screenshot shows a window titled "RADIUS Summary - CNL-422-0-0". Inside the window is a table with the following data:

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

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

- Click **Close**.
- 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:

- From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 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.
- Click the **Auth & Acct** tab.
- 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.
- To save your changes, 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 Identifi Wireless 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 230.

To Define a WLAN Service with No Authentication:

- From the top menu, click **NS Configurat**. The **Virtual Network Configuration** screen displays.
- In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to configure or click **New**. The **WLAN Services** configuration page is displayed.
- Configure the service as described in [WLAN Services Overview](#) on page 243.
- Click the **Auth & Acct** tab.
- From the **Authentication Mode** drop-down list, select Disabled.
- To save your changes, 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 Identifi Wireless 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**. The **Virtual Network Configuration** screen displays.
- 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 Auth & ACCT page displays.

The screenshot shows the configuration page for WLAN: CNL-422-0-0. The 'Auth & Acct' tab is selected. The page includes the following elements:

- Navigation:** Home, Logs, Reports, Controller, AP, VNS, Radar, Help, Logout.
- Left Sidebar:** New..., Global, Sites, Virtual Networks, WLAN Services (selected), CNL-422-0-0, CNL-422-0-1, CNL-422-0-2, CNL-422-0-3, CNL-422-1-2-wds, CNL-422-1-4-wds, CNL-422-1-5, CNL-422-1-6, CNL-422-1-7, CNL-422-2-10, CNL-422-2-11, CNL-422-2-12-wds, CNL-422-2-8, CNL-422-2-9, CNL-422-3-12, CNL-422-3-13, CNL-422-3-14, CNL-422-3-15-wds, CNL-422-WDS, Roles, Classes of Service, Topologies.
- WLAN Services:** WLAN Services, Privacy, **Auth & Acct**, QoS.
- Authentication:** This type of authentication requires the user to be on a bridged at controller or routed topology. Mode: Internal (dropdown), Configure... button. Enable MAC-based authentication, Configure... button.
- RADIUS Servers:** Use (dropdown), Use button. Table:

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"/>

 Buttons: New, Move Up, Move Down, Configure, Test, Summary, Remove, Radius TLVs.
- Accounting:** Collect Accounting Information of Wireless Controller.
- Buttons:** New, Delete, Save.

- 4 In the **Authentication Mode** drop-down list, select a Captive Portal option:

- Disabled
- 802.1x
- Internal
- External
- Firewall Friendly External
- Guest Portal
- Guest Splash

- 5 Click Configure. The Captive Portal configuration page displays. The page display differs depending on the mode selected. See [Figure 28: Captive Portal Page Configuration Page for Internal and Guest Splash Modes](#) on page 272 for Internal and Splash modes, [Figure 29: Captive Portal Page for External and 802.1x Modes](#) on page 272 for External and 802.1x modes, [Figure 30: Captive Portal Page for Guest Portal Mode](#) on page 273 for GuestPortal mode, and [Figure 31: Captive Portal Page for Firewall Friendly External Mode](#) on page 274 for Firewall Friendly External Captive Portal mode. Use the fields and buttons available on each page to configure Captive Ports.

[Table 65: Configure Internal Captive Portal Page - Fields and Buttons](#) on page 274 describes the internal captive portal configuration fields and buttons. [Table 66: External Captive Portal Page - Fields and Buttons](#) on page 276 describes the external captive portal configuration fields and buttons. [Table 67: Firewall Friendly External Captive Portal](#) on page 276 describes the firewall friendly external captive portal configuration fields and buttons. Use these field and button descriptions to configure captive portal.

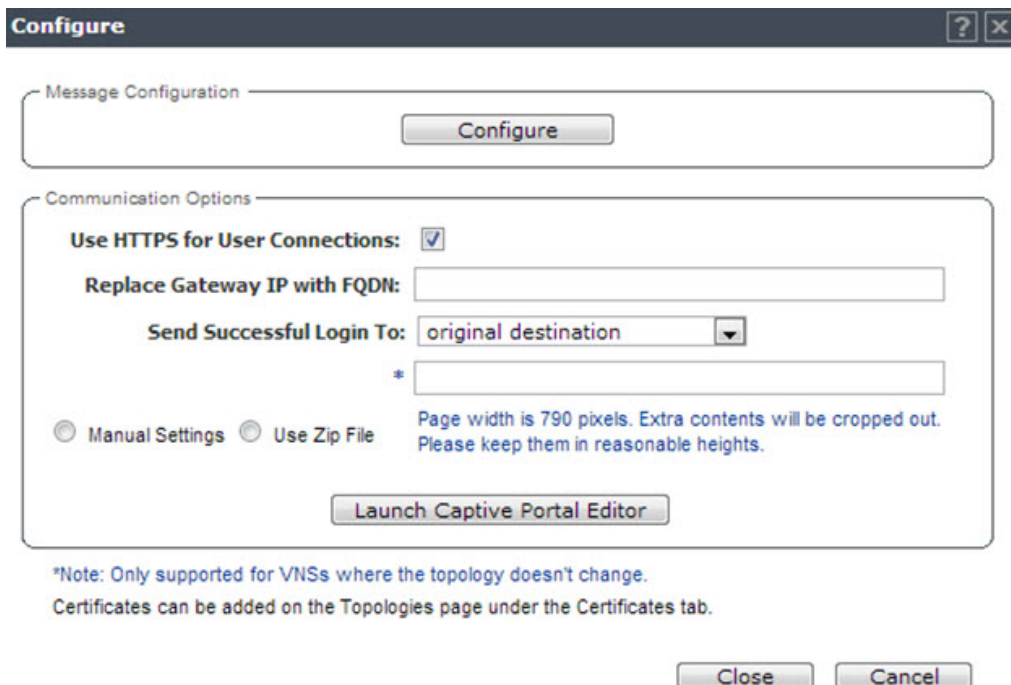


Figure 28: Captive Portal Page Configuration Page for Internal and Guest Splash Modes

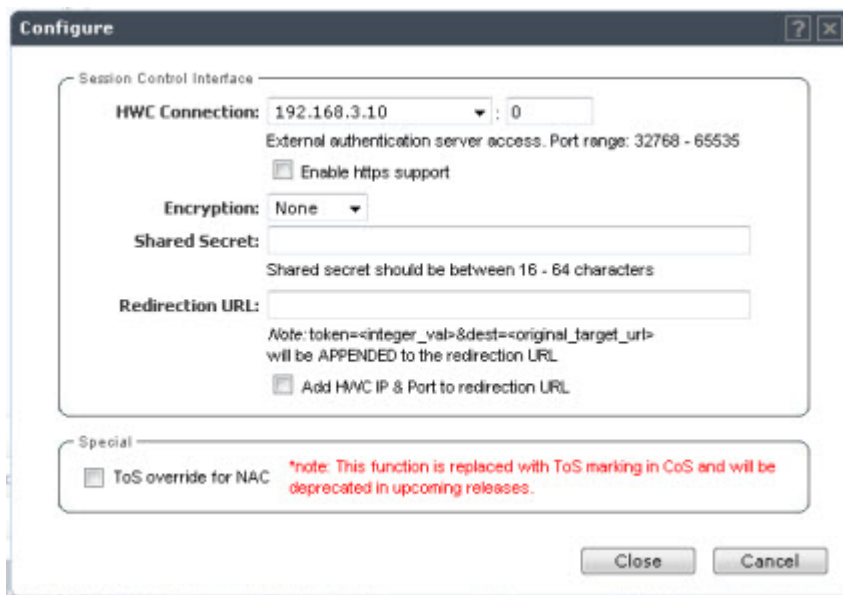


Figure 29: Captive Portal Page for External and 802.1x Modes

The screenshot shows a 'Configure' window with the following sections:

- GuestPortal**:
 - Buttons: Manage Guest Users, Configure Ticket Page
 - Account Lifetime: 30 days (0 = no limit)
 - Guest Admin Can Set Account Lifetime:
 - Maximum Session Lifetime: 0 hours (0 = no limit)
 - User ID Prefix: Guest-
 - Minimum Password Length: 8
- Message Configuration**:
 - Configure
- Communication Options**:
 - Use HTTPS for User Connections:
 - Replace Gateway IP with FQDN:
 - Send Successful Login To: original destination (dropdown)
 - (with asterisk)
 - Manual Settings (selected) / 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 30: Captive Portal Page for Guest Portal Mode

Configure

Redirect to External Captive Portal

Identity:

Shared Secret:

Shared secret should be between 16 - 255 characters

Redirection URL:

Note: token=<integer_val>-sdest=<original_target_url> will be APPENDED to the redirection URL

EWC IP & port
Replace EWC IP with EWC FQDN:

AP name & serial number

Associated BSSID

VNS Name

SSID

Station's MAC address

Currently assigned role

Containment VLAN (if any) of assigned role

Timestamp

Signature

Redirect From External Captive Portal

Use HTTPS for User Connections:

Send Successful Login To:

View Sample Close Cancel

Figure 31: Captive Portal Page for Firewall Friendly External Mode

Table 65: 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 567
Configure Ticket Page	Click to configure the guest portal ticket. The Configure ticket page displays. For information about how guest portal ticket pages and how to activate them, see Working with GuestPortal Administration on page 567.
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.

Table 65: Configure Internal Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
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 (Table 68: Message Configuration Page - Fields and Buttons on page 278).
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.
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.

Table 66: 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.
Encryption	Select the data encryption to use. Options are: <ul style="list-style-type: none"> • None • Legacy • AES
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.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication. Note: The Redirection URL does not support IPv6.
Add EWC IP & Port to redirection URL	Select the checkbox to enable redirection.
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 230.

Table 67: Firewall Friendly External Captive Portal

Field/Button	Description
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.
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.

Table 67: Firewall Friendly External Captive Portal (continued)

Field/Button	Description
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication. Note: The Redirection URL does not support IPv6.
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.
Send Successful Login to:	in the drop-down list, click the IP address of the external Web server. and then enter the port of the controller.

Error Message Configuration

You can configure informational and error messages that a user may encounter when trying to access a captive portal.

To configure the error and informational messages:

- 6 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 7 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 8 Click the **Auth & Acct** tab. The Auth & Accounting page displays.
- 9 In the **Authentication Mode** drop-down list, select a Captive Portal option.
- 10 Click Configure. The Captive Portal Configuration page displays.
- 11 In the Message Configuration section, click the Configure button. The Message Configuration page displays. [Table 68: Message Configuration Page - Fields and Buttons](#) on page 278 describes the message configuration fields and buttons.

The screenshot shows a 'Configure' dialog box titled 'Message Configuration'. It contains several fields, each with a label and a text input area. The fields and their values are:

- Invalid:** Empty id / password
- Success:** Success
- Access Fail:** Userid or password incorrect. Please try again.
- Fail:** A problem has occurred while trying to validate your userid &
- Timeout:** A problem has occurred while trying to validate your userid &
- RADIUS shared security key fail:** A problem has occurred while trying to validate your userid &
- RADIUS internal error:** A problem has occurred while trying to validate your userid &
- Max RADIUS login fail:** Too many users
- Invalid Login parameters:** Userid or password
- General failure:** A problem has occurred while trying to validate your userid &
- Invalid third party parameters:** Invalid third party
- Authentication in progress fail:** Authentication is in

At the bottom of the dialog are two buttons: 'Close' and 'Cancel'.

Table 68: 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.
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.

Table 68: Message Configuration Page - Fields and Buttons (continued)

Field/Button	Description
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 Launch the Captive Portal Editor:

- 12 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 13 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 14 Click the **Auth & Acct** tab. The **Auth & Accounting** page displays.
- 15 In the **Authentication Mode** drop-down list, select a Captive Portal option.
- 16 Click **Configure**. The **Captive Portal Configuration** page displays.
- 17 In the Communications Options section, select **Manual Settings** and then click **Launch Captive Portal Editor**. The Captive Portal Editor page displays. [Table 69: Captive Portal Editor - Fields and Buttons](#) on page 280 describes the captive portal editor fields and buttons.



Note

The Captive Portal Editor page supports only one administrator editing a captive portal page at one time.

Table 69: 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 69: 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

Table 69: Captive Portal Editor - Fields and Buttons (continued)

Field/Button	Description
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.

**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 230.

**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.

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 70: 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 71: 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 71: Relationship Between Service Class and 802.1D UP](#) on page 283. 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 70: Service Classes](#) on page 283. 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 72: 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 73: 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**. The **Virtual Network Configuration** screen displays.
- 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 **QoS** tab.

The screenshot shows the configuration page for a WLAN service named 'ext'. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar shows a tree view with 'WLAN Services' expanded, listing 'ext', 'int', 'mesh', and 'wds1'. The main content area is titled 'WLAN: ext' and has tabs for 'WLAN Services', 'Privacy', 'Auth & Acct', and 'QoS'. The 'QoS' tab is active, showing the following configuration:

- Wireless QoS**
 - WMM
 - 802.11e
 - Turbo Voice
 - U-APSD
- Admission Control**
 - Use Global Admission Control for Voice (VO)
 - Use Global Admission Control for Video (VI)
 - Use Global Admission Control for Best Effort (BE)
 - Use Global Admission Control for Background (BK)

* Global admission controls are configured through Global Settings
- Flexible Client Access**
 - Flexible Client Access may not work if Global Admission Controls for Voice and Video (Advanced QoS settings) are enabled.

Buttons for 'New', 'Delete', and 'Save' are at the bottom. An 'Advanced' button is also present.

Table 74: 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 292.</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 292.</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 74: WLAN Services QoS Tab - Fields and Buttons (continued)

Field/Button	Description
	<p>For more information, see VNS Global Settings on page 292.</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 292.</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 288.</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 74: 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 75: 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 75: 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		

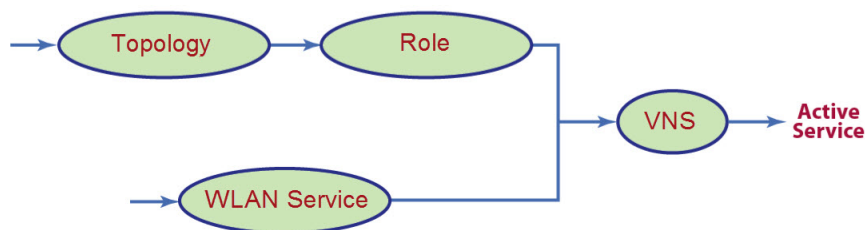
8 Configuring a VNS

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 32: VNS Configuration Flow](#) on page 290 below.

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.



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 tab.
- 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, GuestPortal, 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.

Figure 32: VNS Configuration Flow

Controller Defaults

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

The Extreme Networks IdentifiFi Wireless 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 will 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 CoS 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 filter mode setting.

- Sync Summary

The “Sync Summary” screen provides an overview of the synchronization status of paired controllers. The screen is divided into 4 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 309.

- NAC Integration

NAC Integration provides a list of NAC Servers for use by the controller for passing DHCP 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 310.

- Client Autologin

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 311.

- 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 312.

- Netflow/MirrorN

The wireless controller leverages and integrates with the Purview solution for decoding, detection, collect (Metadata) and scrutinize layer 7 data. The solution functions by first enabling WLANs on wireless controller to forward Netflow to a Purview engine. This provides all the standard information found in a Netflow v9 packet including source and destination IP addresses and ports along with protocol and packet counter information. For more information, see [Using Netflow/MirrorN](#) on page 313.

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**. The **Virtual Network Configuration** screen displays.

- 2 In the left pane, click **Global** > **Authentication**.
- 3 To enable changing RADIUS server settings per WLAN Service, select **Strict Mode**.

The screenshot shows the VNS configuration interface. The left sidebar contains a navigation menu with the following items: New..., Global, Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, Netflow/MirrorN, Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The 'Global' menu is expanded, and 'Authentication' is selected. The main content area is titled 'RADIUS Servers' and shows 'RFC 3580 (ACCESS-ACCEPT) Options'. A checkbox for 'Strict Mode' is checked. Below this is a table with columns: Server, Default, Retries, Timeouts, Ports, and Priority. The table contains one entry with Alias 'r1', Hostname/IP '11.11.11.11', Protocol 'PAP', Retries '3', Acct '3', Timeouts '5', Acct '5', Ports '1812', Acct '1813', and Priority '1'. Below the table is a note: '* RADIUS servers which are currently associated with WLAN Service(s) cannot be removed'. There are 'New' and 'Delete Selected' buttons. Below that is a 'MAC Address' section with a dropdown menu showing 'XXXXXXXXXXXX'. An 'Advanced...' button is at the bottom right, and a 'Save' button is at the very bottom.

- 4 To define a new RADIUS server available on the network, click **New**. The **RADIUS Settings** dialog displays.

The screenshot shows the 'RADIUS Settings' dialog box. The title bar says 'RADIUS Settings' with a help icon and a close icon. The main title is 'RADIUS Server'. The form has the following fields and sections:

- Server Alias:** [text input]
- Hostname IP:** [text input]
- Shared Secret:** [text input] with an 'Unmask' button to its right.
- Default Protocol:** [dropdown menu] showing 'PAP'.
- Authentication section:**
 - Priority:** [text input] with value '2'.
 - Total Number of Tries:** [text input] with value '3'.
 - RADIUS Request Timeout:** [text input] with value '5' and '(seconds)' to its right.
 - Port:** [text input] with value '1812'.
- Accounting section:**
 - Priority:** [text input] with value '2'.
 - Total Number of Tries:** [text input] with value '3'.
 - RADIUS Request Timeout:** [text input] with value '5' and '(seconds)' to its right.
 - Interim Accounting Interval:** [text input] with value '30' and '(minutes)' to its right.
 - Port:** [text input] with value '1813'.
 - Send Interim Accounting Records for:** [checkbox]
 - Fast Fallback Events:** [checkbox]

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

- 5 In the **Server Alias** box, 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 78.

- 6 In the **Hostname/IP** box, 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 95.

- 7 In the **Shared Secret** 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.

Note

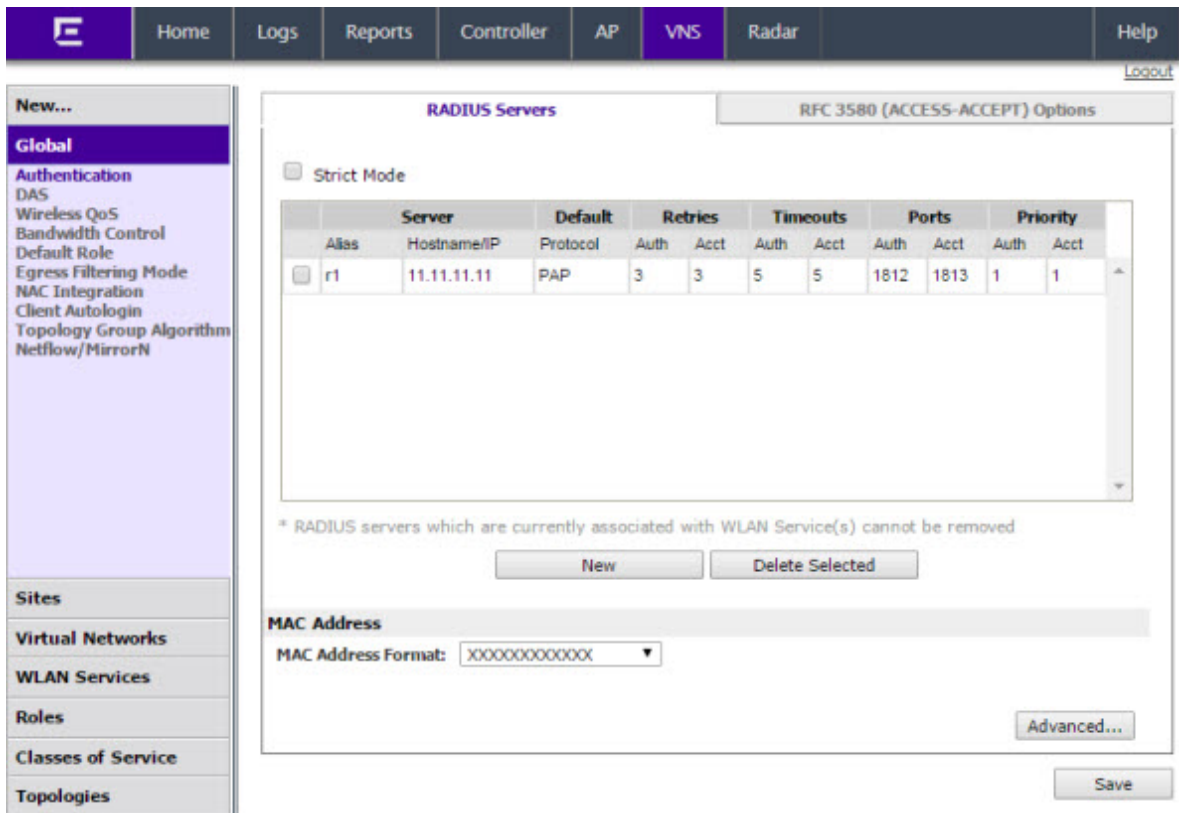


You should always proofread your Shared Secret key to avoid any problems later when the controller attempts to communicate with the RADIUS server.

- 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.
 - Port — default Authentication port is 1812. Default Accounting port is 1813.
 - Send Interim Accounting Records for —

Fast Failover Events: default is unchecked. Select to send interim records immediately from the controller receiving the session.
 - For Accounting operations, the Interim Accounting Interval — default is 30 minutes.
- 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.



The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A sidebar on the left lists various configuration categories under 'New...' and 'Global', including 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 shows a table with columns for Alias, Hostname/IP, Protocol, Retries (Auth, Acct), Timeouts (Auth, Acct), Ports (Auth, Acct), and Priority (Auth, Acct). A single server 'r1' is listed with Hostname/IP 11.11.11.11, Protocol PAP, and Retries of 3 for both Auth and Acct. Below the table, there is a 'MAC Address' section with a dropdown menu for 'MAC Address Format' set to 'XXXXXXXXXXXX'. A 'Save' button is located at the bottom right of the interface.

Alias	Server	Default	Retries		Timeouts		Ports		Priority		
			Auth	Acct	Auth	Acct	Auth	Acct	Auth	Acct	
<input type="checkbox"/>	r1	11.11.11.11	PAP	3	3	5	5	1812	1813	1	1



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**. The **Virtual Network Configuration** screen displays.
- 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**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global**, then **Authentication**.
- 3 In the **MAC Address** area, click **Advanced**.

- 4 The Advanced dialog displays.

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:

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.

Close

To Include the SERVICE-TYPE Attribute in the Client ACCESS-REQUEST Messages:

- 5 Select **Include Service-Type attribute in Client Access Request messages**.
- 6 Click **Close**.
- 7 Click **Save** to save your changes.

To Enable RADIUS Accounting:

- 8 Select **RADIUS Accounting**.



Note

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.

To Specify Authentication Behavior of RADIUS servers on Server Failure

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. If authentication to the primary server fails, the client authentication is transferred to the backup server. Clients remain authenticating on the last working RADIUS server, but once the primary server has recovered, the administrator can bring the client authentication back to the primary server.

- 9 Under **How should multiple RADIUS servers be used?**, for Authentication, select one of the following options:
 - Send requests to Primary whenever it is up (Primary-Backup).
 - Send request to one server until it fails (Round-Robin).
- 10 Click **Close**.

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**. The **Virtual Network Configuration** screen displays.
- 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. There are three 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**.

- 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. A left sidebar contains a 'New...' menu with 'Global' selected, and sub-menus for Authentication, Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main content area is titled 'RFC 3580 (ACCESS-ACCEPT) Options' and contains the following text:

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.

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

- 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**.
- 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.

The screenshot shows the VNS configuration interface with the 'RFC 3580 (ACCESS-ACCEPT) Options' tab selected. The configuration options are the same as in the previous screenshot. A 'Vlan ID Role Mapping' table is visible, which is currently empty. Below the table are 'New' and 'Delete Selected' buttons.

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
?
✕

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.

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
?
✕

Vlan ID: (1-4094)

Role:

- 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 NAC or another third-party application, including RADIUS applications. For more information, see [NAC integration with Extreme Networks Wireless WLAN](#) on page 31.

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**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global > DAS**.

- 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.

- 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 302
- [Configuring QoS Flexible Client Access](#) on page 303

Configuring QoS Admission Control Thresholds

To Define Admission Control Thresholds for VNS Global Settings:

- From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- In the left pane, click **Global** > **Wireless QoS**.

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 visible in the top right corner. The left sidebar shows a tree view with 'Global' selected, containing sub-items: Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, and Netflow/MirrorN. 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'.

The section below is titled 'Flexible Client Access' and contains the following setting:

- Fairness Policy: 100% Airtime

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

- 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 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.

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**.

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 'New...' button and a tree view with 'Global' selected, showing sub-items like Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, and Netflow/MirrorN. 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 several settings with dropdown menus:

- 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%

Below these settings is a note: 'Note: Settings only apply on APs serving QoS-enabled WLAN Service with Admission Control enabled'. Under the 'Flexible Client Access' section, there is a 'Fairness Policy' dropdown set to '100% Airtime'. A 'Save' button is located at the bottom right of the configuration area.

- 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**.

The screenshot shows the 'Virtual Network Configuration' interface. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar is expanded to 'Global' > 'Bandwidth Control', with a list of sub-items: Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, and Netflow/MirrorN. Below this are sections for Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main content area is titled 'Bandwidth Control Profiles' and features a list box (currently empty), a 'Remove selected profile' button, and an 'Add new profile' button. To the right, there are input fields for 'Profile Name:' and 'Average Rate (CIR):' (with a 'kbps' unit), and a 'Save Profile' button. A 'Save' button is located at the bottom right of the main area.

- 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.

- 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 212.

- 5 Select an Invalid Role Action from the one of the following:

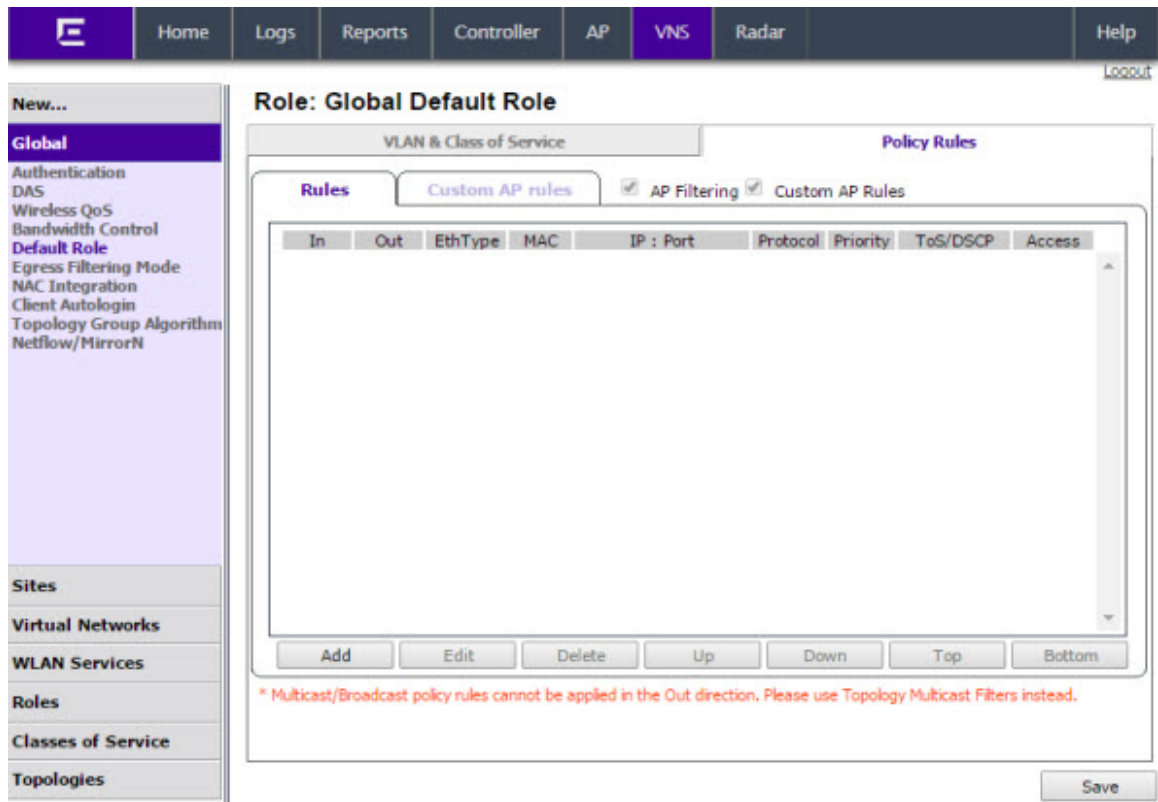
- Select **Apply Default Role**.
- Select **Allow All traffic**.
- Select **Deny All traffic**.

- 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.



- 2 To add a rule, click **Add**. The fields in the Add Filter area are enabled.
- 3 Configure the fields as desired. For more information, see [Policy Rules](#) on page 230.
- 4 To configure custom AP filters, select the **AP Filtering** checkbox, then select the **Custom AP Rules** checkbox and click the **Custom AP rules** tab. Then configure the rules as desired.

For more information, see [Defining Policy Rules for Wireless APs](#) on page 235.

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 Extreme Networks Identifi Wireless 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 filter mode setting. By default the global egress filtering mode is set to Use WLAN setting. In this mode, egress filtering can be enabled for some WLAN services and not others, by using the Egress Filtering Mode setting available in each WLAN service's Advanced configuration dialog.

Changing the global egress filtering mode doesn't alter each individual WLAN service's own egress filtering mode setting, although it can override them. Changing the global egress filtering mode doesn't 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 will affect how a role's rules are interpreted when they are applied.

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 > Egress Filtering Mode**. The **Egress Filtering Mode Configuration** screen displays.

The screenshot shows the VNS interface with the 'VNS' menu item selected. The left sidebar contains a navigation tree with 'Global' selected, and 'Egress Filtering Mode' highlighted. 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 *
- Use WLAN Service setting

At the bottom of the configuration area, there is a red asterisk note: "* When "In" filter rules are applied to "Out" traffic, the role of the source and destination address are reversed". A 'Save' button is located at the bottom right of the configuration area.

- 3 In the Egress Filtering Mode Configuration area select an egress filtering mode:
- When egress filtering mode is set to **All WLAN Services enforce explicitly defined “Out” rules**, all WLAN services will enforce outbound filters on egress traffic, exactly as they are defined in the role.
 - When egress filtering mode is set to **All WLAN Services apply “In” policy rules to “Out” direction traffic**, all WLAN services will enforce that any outbound policy rules 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.
 - When egress filtering mode is set to **Use WLAN Service setting**, each role’s rules will be 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



It is recommended that this setting be left at **Use WLAN Service setting**. 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.

Using the Sync Summary

The Sync Summary screen provides an overview of the synchronization status of paired controllers.

The screenshot shows the Sync Summary screen with the following data:

Name	Sync	Status
dshjkal	<input checked="" type="checkbox"/>	Synchronized
gfdsgf	<input checked="" type="checkbox"/>	Synchronized
site3	<input checked="" type="checkbox"/>	Synchronized

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 checked="" type="checkbox"/>	Failed

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:

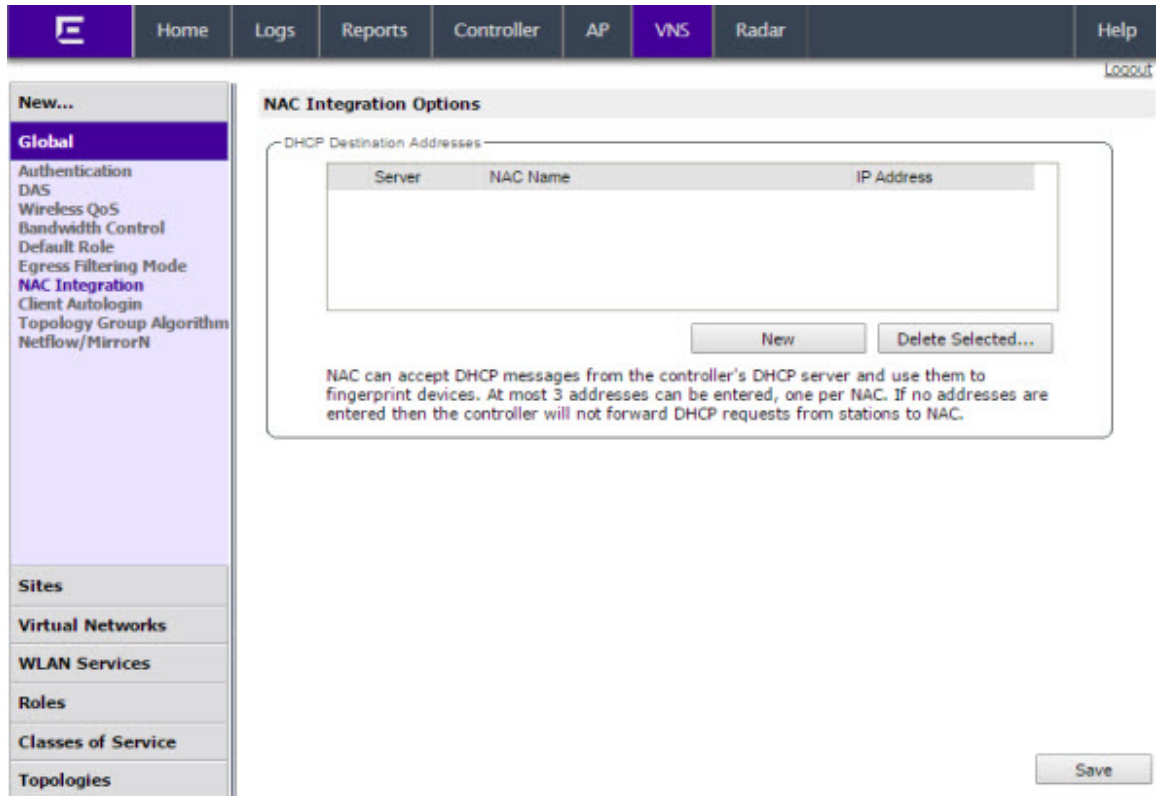
- Synchronized
- Not Synchronized
- Failed
- Conflict (with a button called “Resolve”)

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 DHCP 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.



Adding a New NAC Server Destination

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global > NAC Integration**. The **NAC Integration Options** screen displays.
- 3 Click **New**. The **NAC DHCP Receiver Address** dialog appears.

- 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 DHCP 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.

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 menu lists various configuration categories, with 'Client Autologin' selected. The main content area is titled 'Client Autologin Handling' and contains the following text: 'Many devices such as those made by Apple implement an autologin feature that prompts the user to login as soon as the device detects the presence of a Captive Portal. These features sometimes cause problems for users who actually interact with the captive portal.' Below this text are three radio button options: 'Hide the captive portal from Autologin detector' (unselected), 'Redirect detection messages to the Captive Portal' (selected), and 'Drop detection messages' (unselected). A 'Save' button is located at the bottom right of the configuration area.

Selecting a Client Autologin option

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 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.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A sidebar on the left lists various configuration categories: New... (Global, Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Egress Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, Netflow/MirrorN), Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main content area is titled "Topology Group Selection Algorithm" and describes the algorithm for selecting a member topology from a topology group. It lists four options: MAC-Based (selected), Round Robin, Random Selected, and Least Used. A "Save" button is located at the bottom right of the configuration area.

The following algorithms are available for selecting a member topology from a Topology Group:

- **MAC Based:** This algorithm always assigns a MAC to the same 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

The wireless software leverages and integrates with the NetSight Purview solution for decoding, detection, collect (Metadata) and scrutinize Layer 7 data. The solution functions by first enabling WLANs on wireless controller to forward Netflow to a Purview engine. This provides all the standard information found in a Netflow v9 packet including source and destination IP addresses and ports along with protocol and packet counter information. The second step is to enable a special policy mirror (aka MirrorFirstN mirror) on the same interfaces to copy and forward the first packets (1 to 31, default is 15) of each new flow to the Purview engine where the application stream is assembled and fingerprints are applied to identify the applications. This information is then combined with the corresponding Netflow record. The newly combined record provides not only IP and TCP/UDP information but also supplies application name and categorization, TCP and application response times as well as application metadata such as URL, User-Agent, SSL certificate or URI information in the case of http and https traffic.

The screenshot shows the 'Netflow/MirrorN Configuration' page. The navigation menu on the left includes 'Global', 'Authentication', 'DAS', 'Wireless QoS', 'Bandwidth Control', 'Default Role', 'Egress Filtering Mode', 'NAC Integration', 'Client Autologin', 'Topology Group Algorithm', 'Netflow/MirrorN', 'Sites', 'Virtual Networks', 'WLAN Services', 'Roles', 'Classes of Service', and 'Topologies'. The configuration form on the right has the following fields:

- Netflow Export-Destination IP Address: 0.0.0.0
- Netflow Export Interval: 60 (30-360 seconds)
- Mirror first N: 15 (1-31 packets/flow)
- Traffic Mirror L2 Port: None

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

The following configuration items are supported:

- **Netflow Export-Destination IP Address:** Configure the purview engine the 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 controller. The default value is None. The other l2ports will only allow to be selected, when it's not referred elsewhere (lag, topologies).

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 **VNSVNS Configuration**. 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 configuration page for VNS: CNL-422-0-0. The left navigation pane is expanded to 'Virtual Networks', listing various VNS instances. The main content area is titled 'VNS: CNL-422-0-0' and has a 'General' tab selected. The configuration is organized into sections: 'Core' with a 'VNS Name' field set to 'CNL-422-0-0'; 'WLAN Service' with a dropdown menu set to 'CNL-422-0-0' and 'Edit' and 'New' buttons; 'Default Roles' with two entries: 'Non-Authenticated' (dropdown: 'CNL-422-0-0-non-authenticated', buttons: 'Edit', 'New', details: 'Action:4090 Class of Service: COS_low BW_low BW_Legacy') and 'Authenticated' (dropdown: 'CNL-422-0-0-default', buttons: 'Edit', 'New', details: 'Action:4090 Class of Service: COS_high BW_high BW_Legacy'); and 'Status' with an 'Enable:' checkbox checked. At the bottom, there are 'New', 'Delete', and 'Save' buttons.

- 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 244.
- 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 290.
- Configure the Status parameters for the VNS:
 - Synchronize** — Enable automatic synchronization with its availability peer. Refer to [Using the Sync Summary](#) on page 309 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 317.
- **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 319.
- **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 327.
- **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 337.

The VNS type dictates the configuration information that is required during the VNS creation process.

Creating a NAC VNS Using the VNS Wizard

The Identifi Wireless 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 Extreme Networks Wireless WLAN](#) on page 31.

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 Identifi Wireless 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 Identifi Wireless Controller is bridged for the VNS.
- **Port** — Physical L2 port to which the configured VLAN is attached.
- **RADIUS server** — IP address of the Extreme Networks 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 Extreme Networks 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**. 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 NAC SSID-based VNS.
- In the **Category** drop-down list, click **NAC VNS**, and then click **Next**. The **NAC-compatible SSID-based VNS** screen displays.

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:

NAC web server IP:

Table 76: NAC-compatible VNS Page - Fields and Buttons

Field/Button	Description
IP Address	Type the IP address of the Identifi Wireless 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 Identifi Wireless 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 Identifi Wireless 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 Identifi Wireless 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**.
- 7 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 377.

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.

- 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 77: 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 77: 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 DHCP	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 78: 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 79: 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 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 — 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)

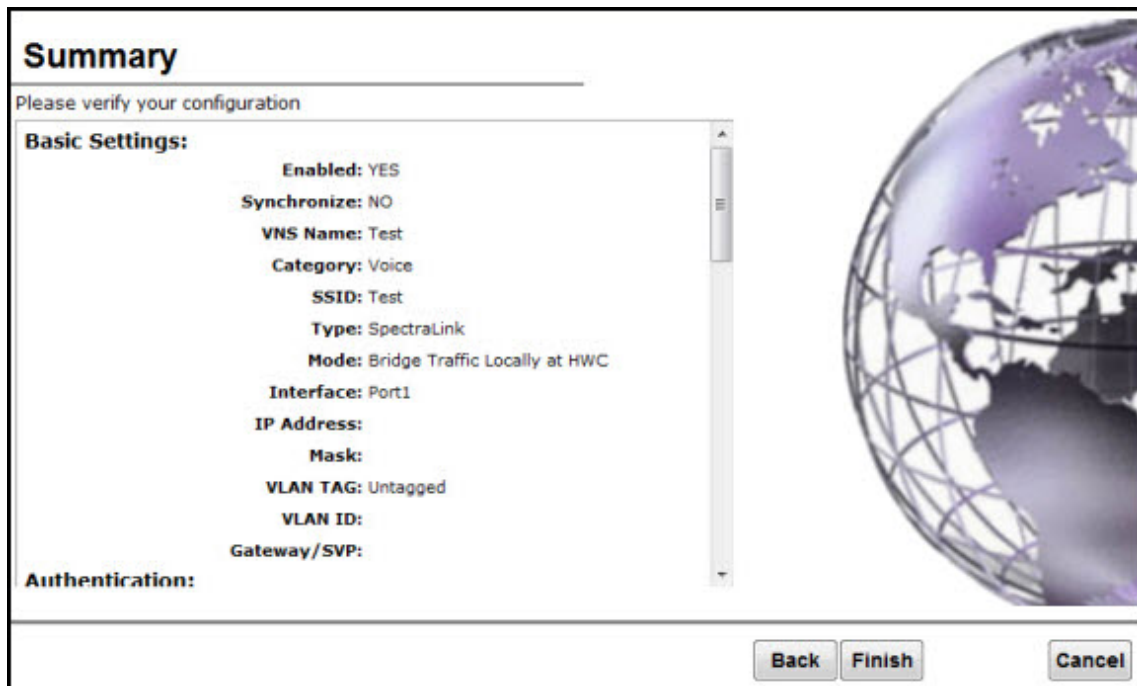
Table 80: Voice VNS Radio Assignment Page - Fields and Buttons

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.

- 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:

Table 81: 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 DHCP	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 81: 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:

Authentication
Test, Data, 802.1x

Radius Server: Add New Server ▾

Server Alias:

Hostname/IP:

Shared Secret: Unmask

Roles: Authentication
 MAC-based Authentication
 Accounting

(Next: DHCP) Back Next Cancel

Table 82: 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 DHCP 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)

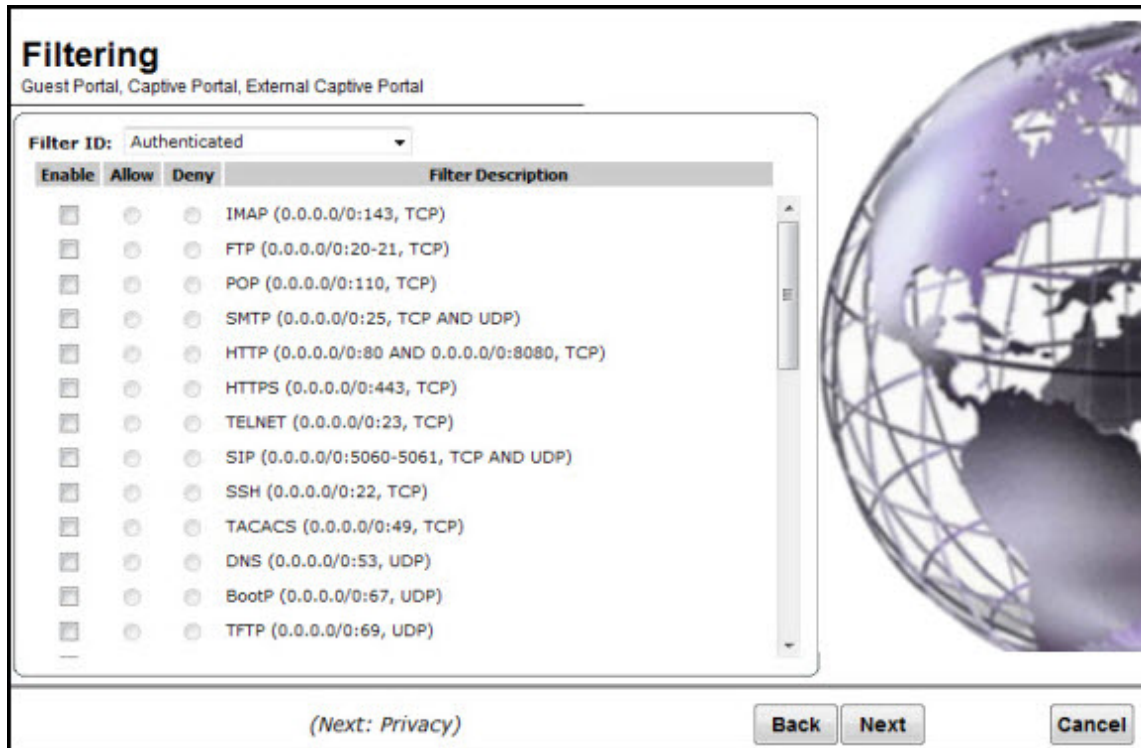
Table 83: Data VNS DHCP Page - Fields and Buttons

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 84: 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 AP36XX and 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 84: 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 AP36XX and 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)

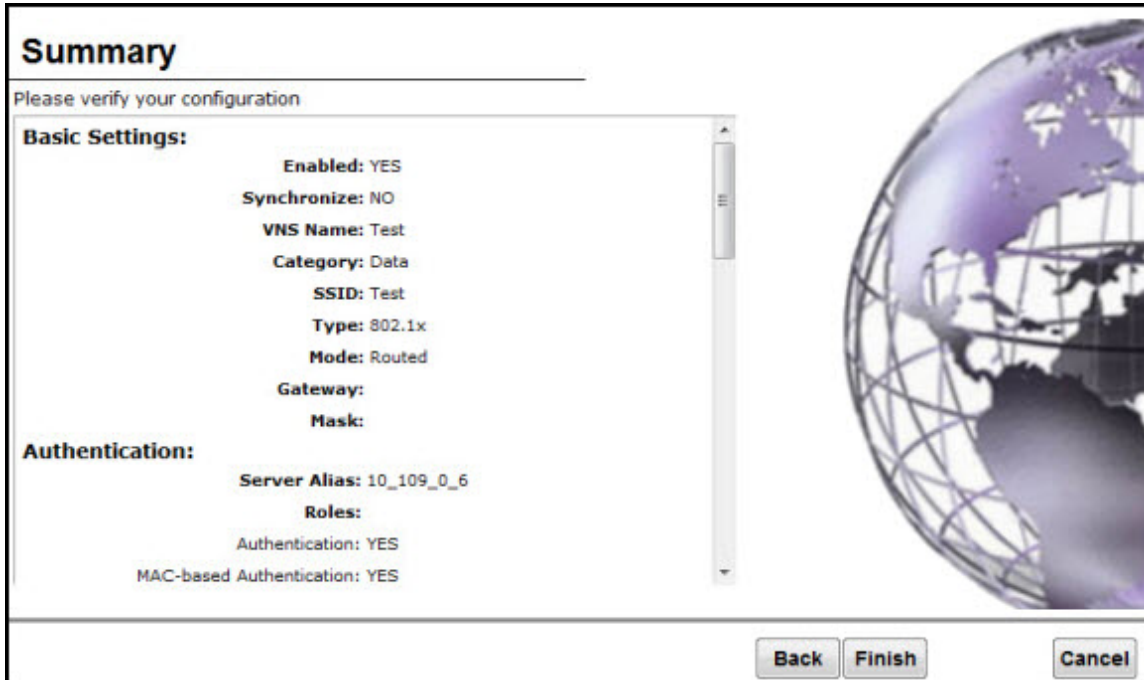
Table 85: Data VNS Radio Assignment Page - Fields and Buttons

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

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 430 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
- DHCP settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary review

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:

Table 86: 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
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).

Table 86: Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
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 DHCP 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 87: 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:

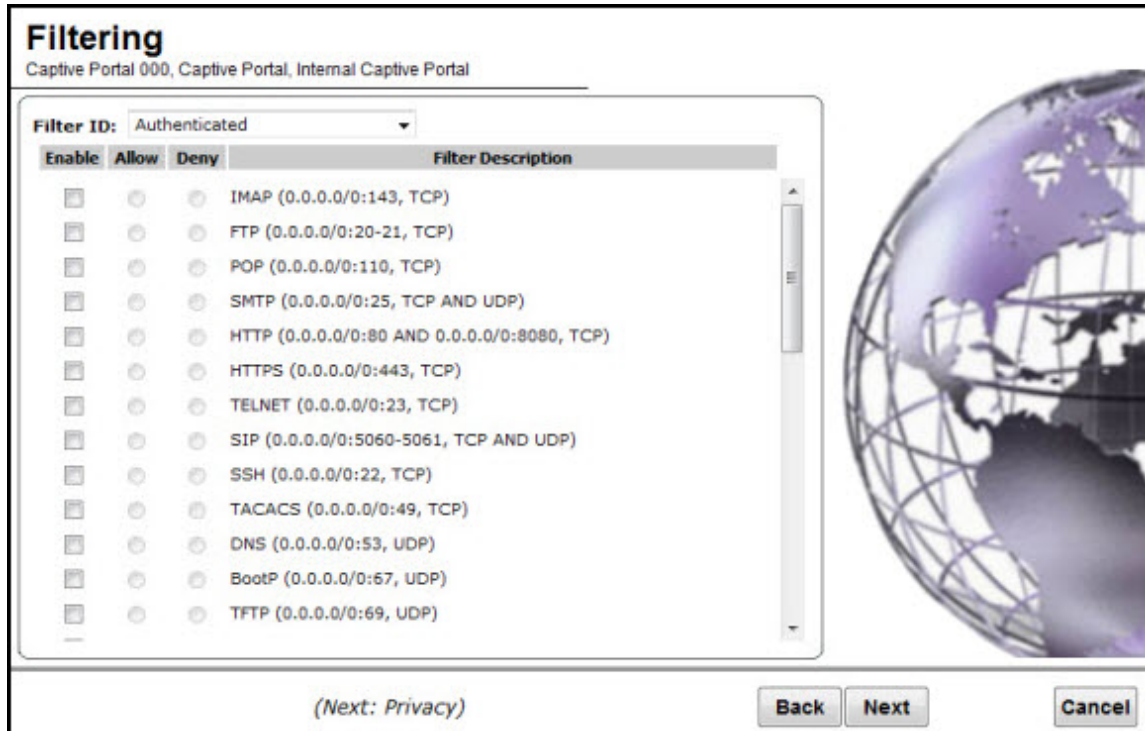
Table 88: Captive Portal DHCP Page - Fields and Buttons

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 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 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 IdentifiFi Wireless 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 89: 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 AP36XX and 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 AP36XX and 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)

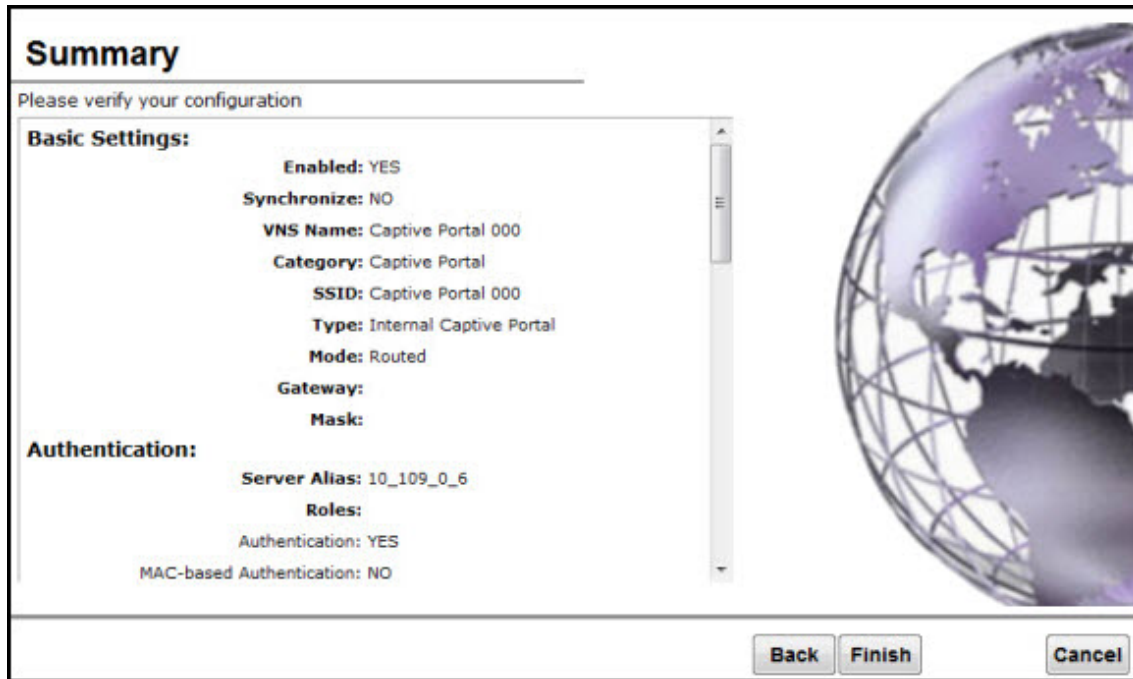
Table 90: Captive Portal Radio Assignment Page - Fields and Buttons

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:



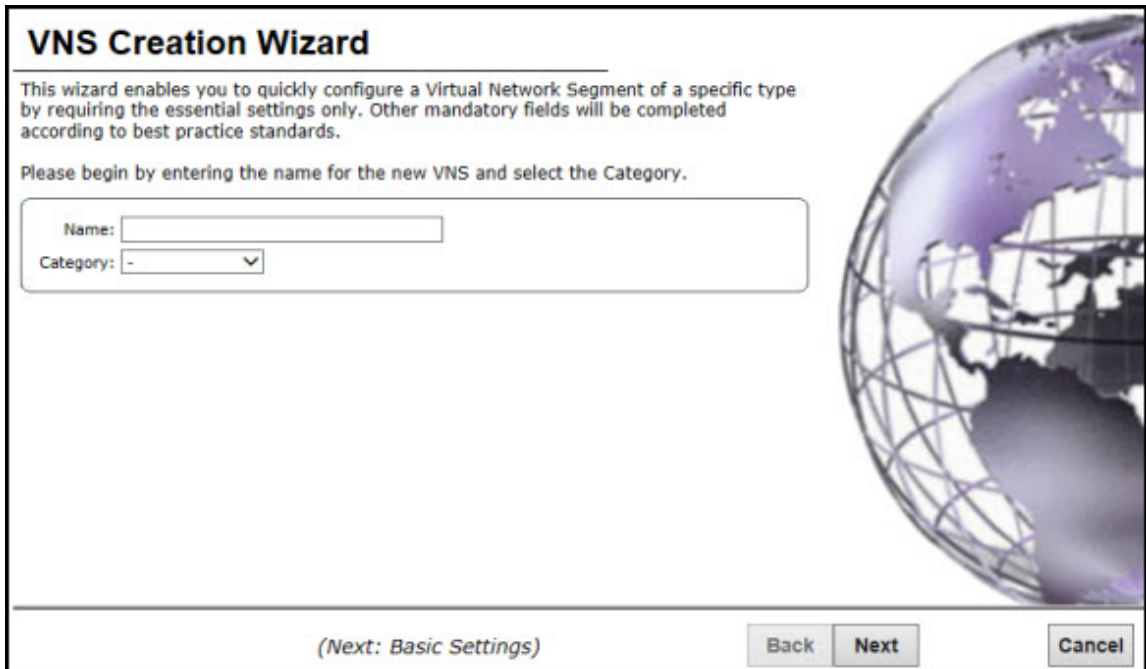
- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

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:

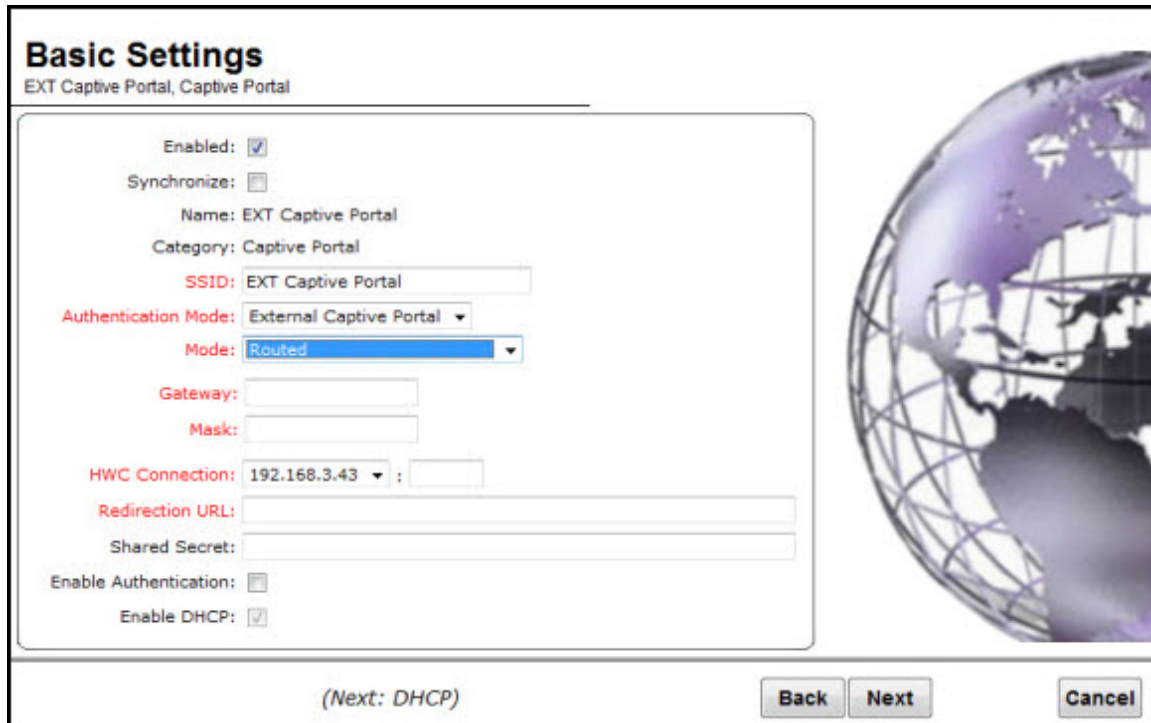
Category:

(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 91: 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.
Routed External Captive Portal	

Table 91: 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).
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 DHCP 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 91: 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.

Authentication
EXT Captive Portal, Captive Portal, External Captive Portal

Radius Server: Add New Server ▾

Server Alias:

Hostname/IP:

Shared Secret: Unmask

Roles: Authentication
 MAC-based Authentication
 Accounting

(Next: DHCP)

Table 92: 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 92: 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)

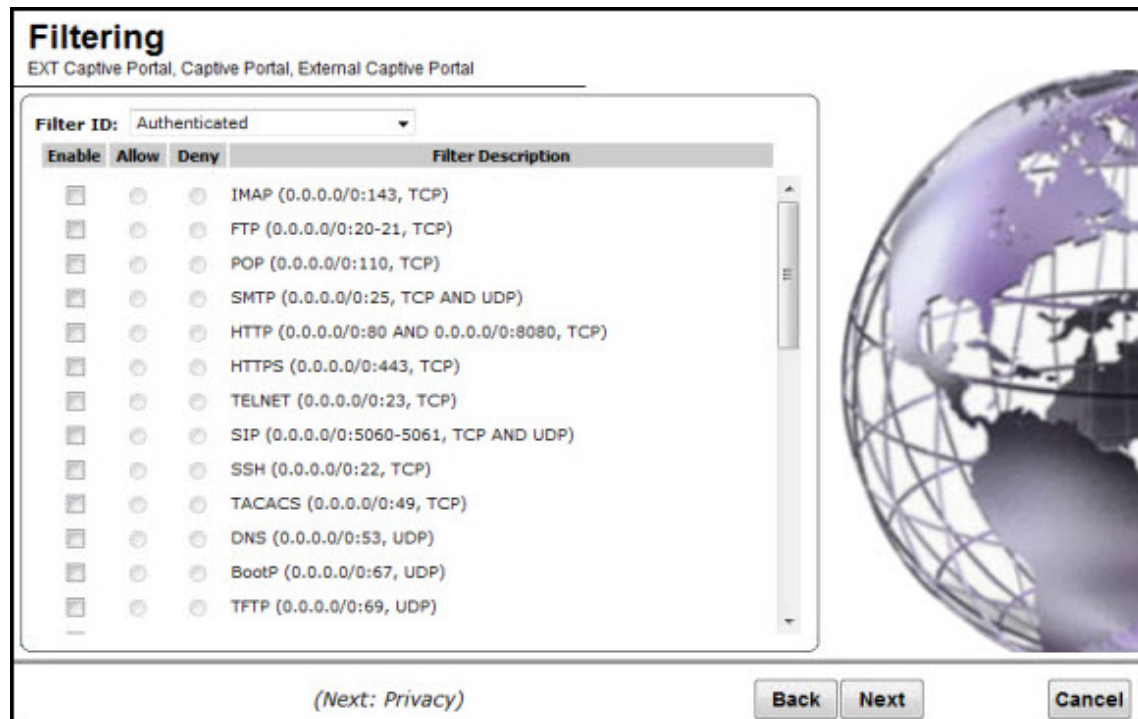
Table 93: External Captive Portal DHCP Page - Fields and Buttons

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 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 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:

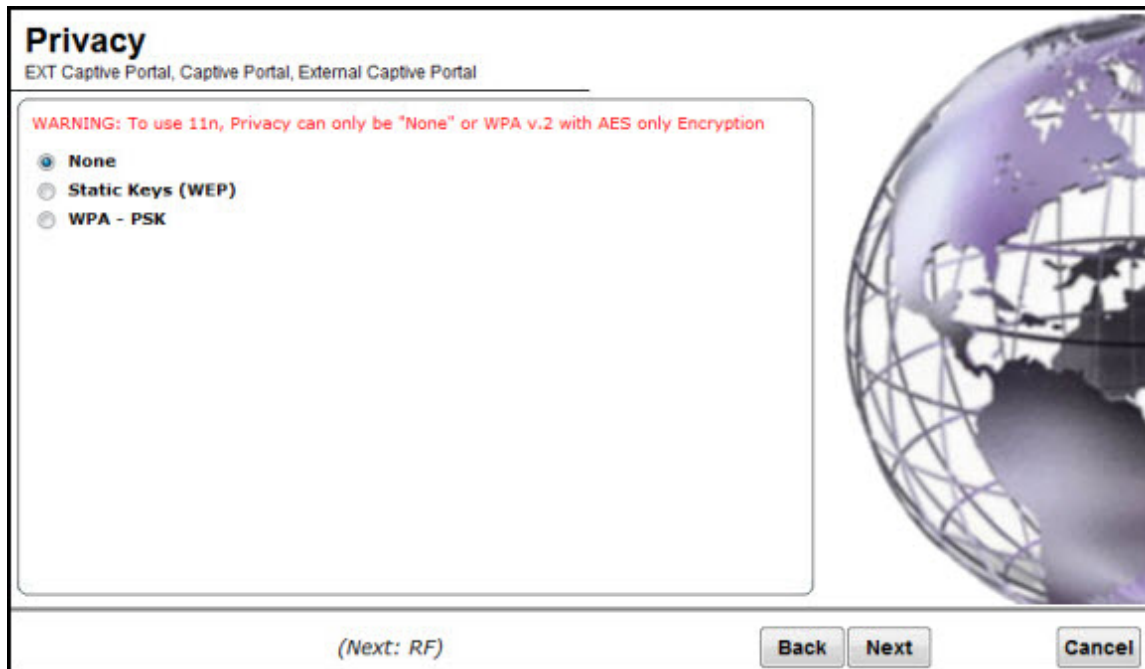


Table 94: External Captive Portal Privacy Page - Fields and Buttons

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 AP36XX and 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 AP36XX and AP37XX Wireless APs.</p>

Table 94: 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:

Radio Assignment
EXT Captive Portal, Captive Portal, 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	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 95: 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 95: 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:

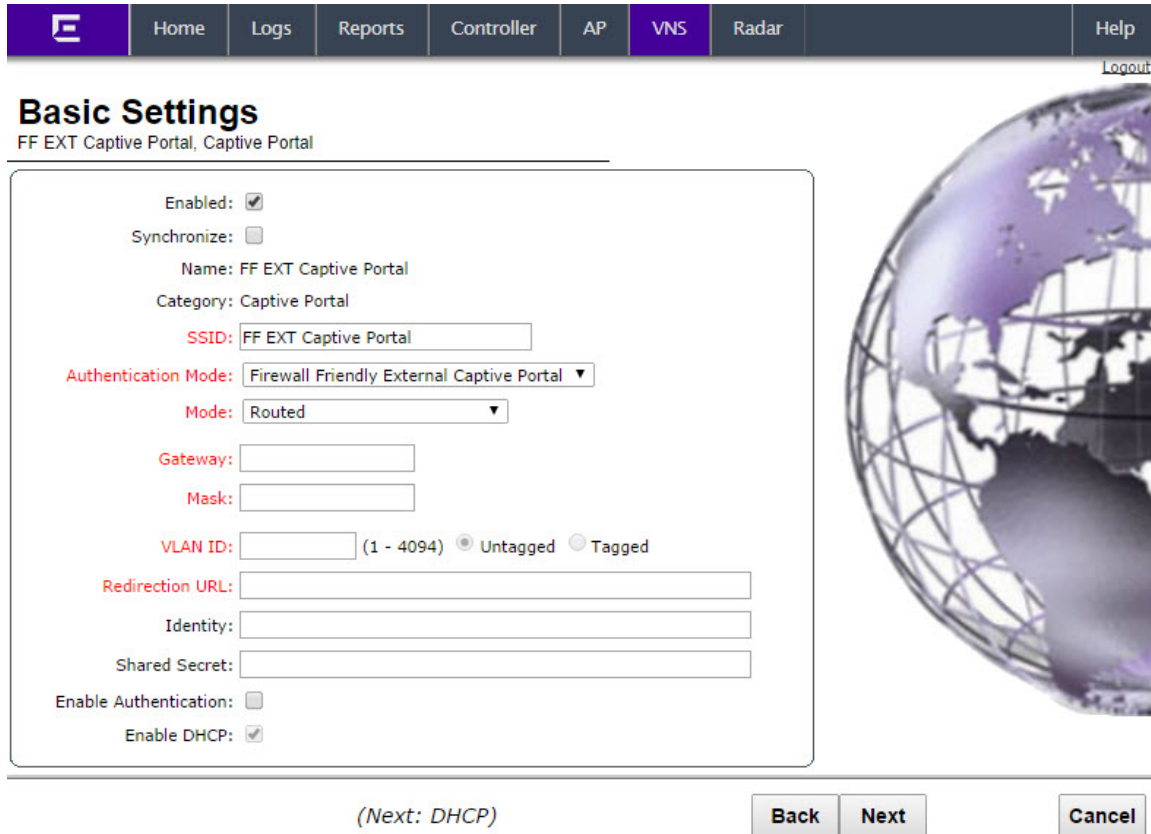
- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the **New** pane, then click **START VNS WIZARD**. The **VNS Creation Wizard** screen displays.

- 3 In the **Name** box, type a name for the 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 96: 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 96: 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 DHCP 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.

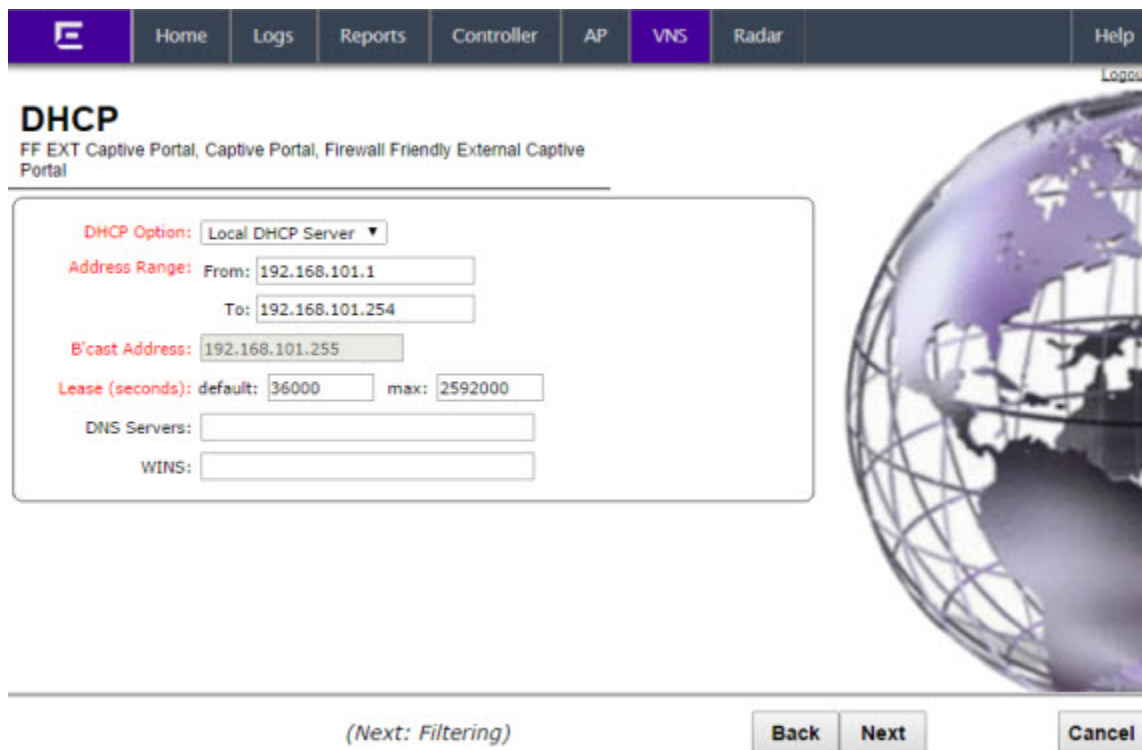
Table 97: Firewall Friendly External Captive Portal Authentication Page - Fields and Buttons

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:



The screenshot shows a web interface for configuring a VNS. The top navigation bar includes links for Home, Logs, Reports, Controller, AP, VNS (highlighted), Radar, and Help. A Logout link is also present. The main heading is "DHCP" with sub-headings "FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal". The configuration form includes the following fields:

- DHCP Option:** Local DHCP Server (dropdown menu)
- 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:** (empty text input)
- WINS:** (empty text input)

At the bottom of the form, there is a note "(Next: Filtering)" and three buttons: Back, Next, and Cancel. A globe graphic is visible on the right side of the interface.

Table 98: 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 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 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: Authenticated

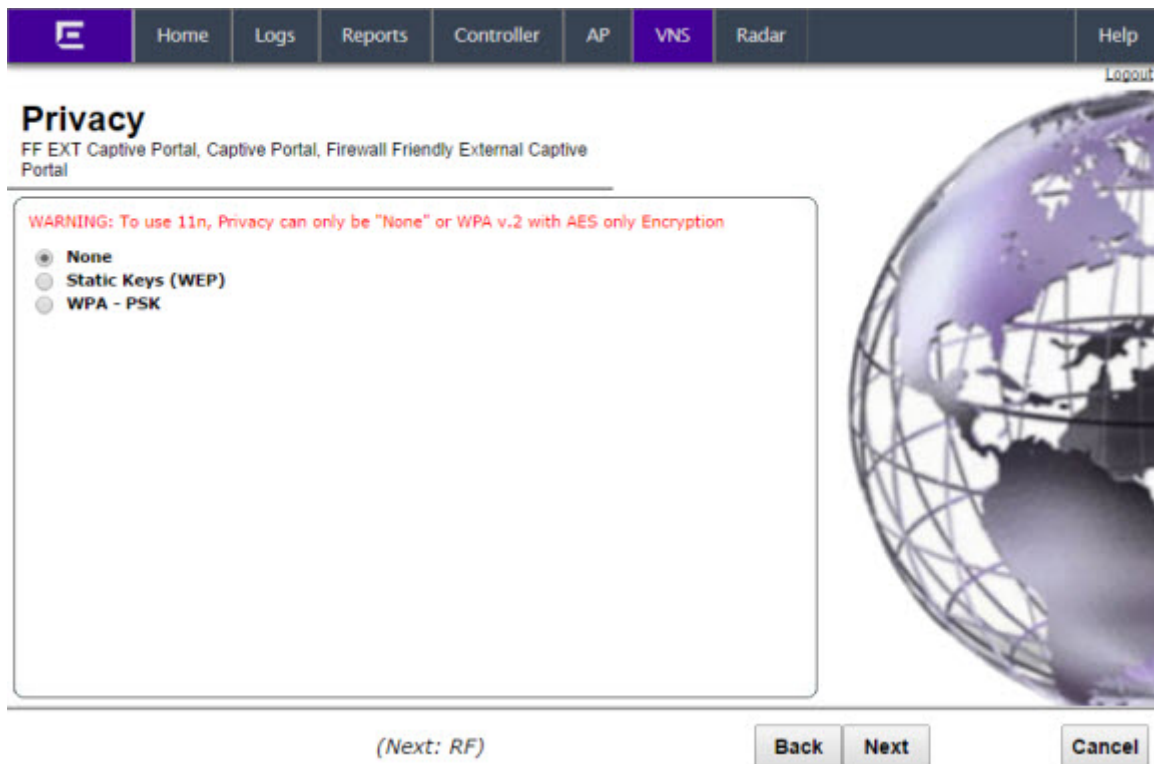
Enable	Allow	Deny	Filter Description
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	IMAP (0.0.0.0/0:143, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	FTP (0.0.0.0/0:20-21, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	POP (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"/>	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) **Back** **Next** **Cancel**

- 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 sub-headings "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". On the right side of the page, there 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 main 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 99: 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 AP36XX and 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 AP36XX and 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 99: 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) **Back** **Next** **Cancel**

Table 100: 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 100: 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 (highlighted), 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 567

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
- DHCP 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 GuestPortal Ticket Page](#) on page 577.
- 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 430.
- 4 Create GuestPortal manager and user accounts.
For more information, see [Working with GuestPortal Administration](#) on page 567
- 5 Manage your guest accounts and GuestPortal logs.
For more information, see the Extreme Networks *IdentiFi Wireless 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.

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)

- 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: Guest-Portal

Authentication Mode: GuestPortal

Mode: Routed

Gateway:

Mask:

Enable DHCP:

(Next: DHCP)

Back Next Cancel

Table 101: 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 101: 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 DHCP.

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) Back Next Cancel

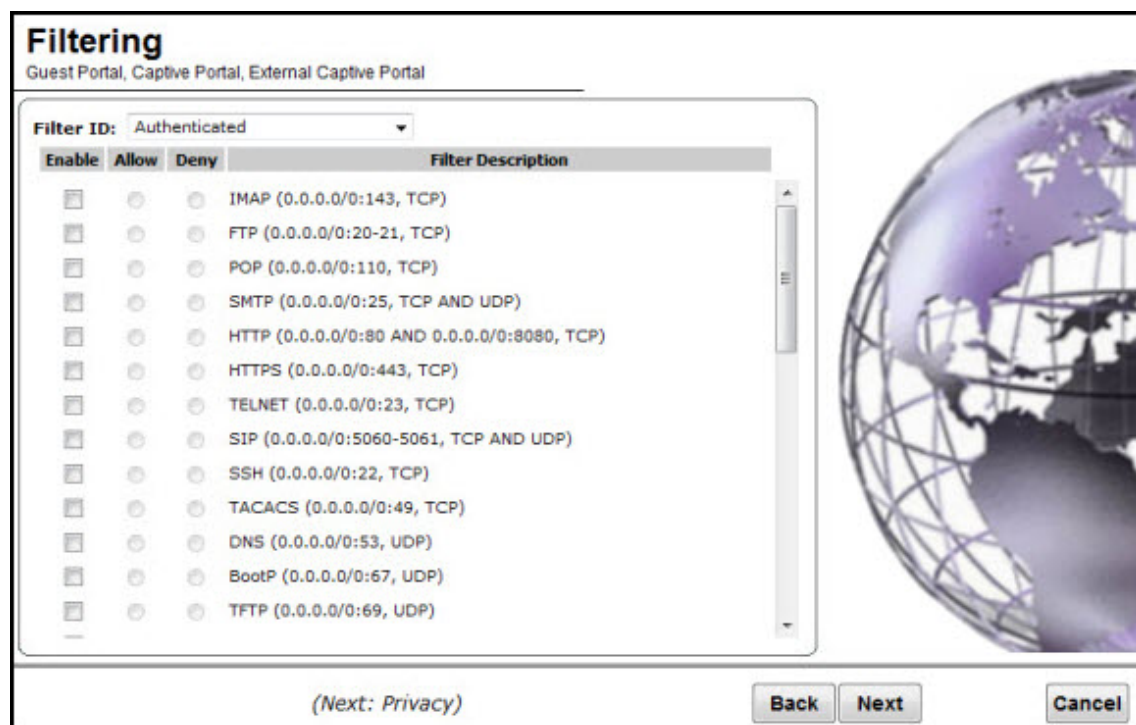
Table 102: Guest Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	<p>In the DHCP Option drop-down list, click one of the following:</p> <p>Use DHCP Relay — Using 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.</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:



- 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)

Table 103: 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 103: 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
 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:
(min 8 characters; max 63)

(Next: RF)

Table 104: 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 AP36XX and 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 AP36XX and AP37XX wireless APs.</p>

Table 104: 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 105: IdentifiFi Wireless 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	64	128

To Enable or Disable a VNS:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 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**. The **Virtual Network Configuration** screen displays.
- 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**. The **Virtual Network Configuration** screen displays.
- 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, Class of Service (CoS) refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a 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 228.

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

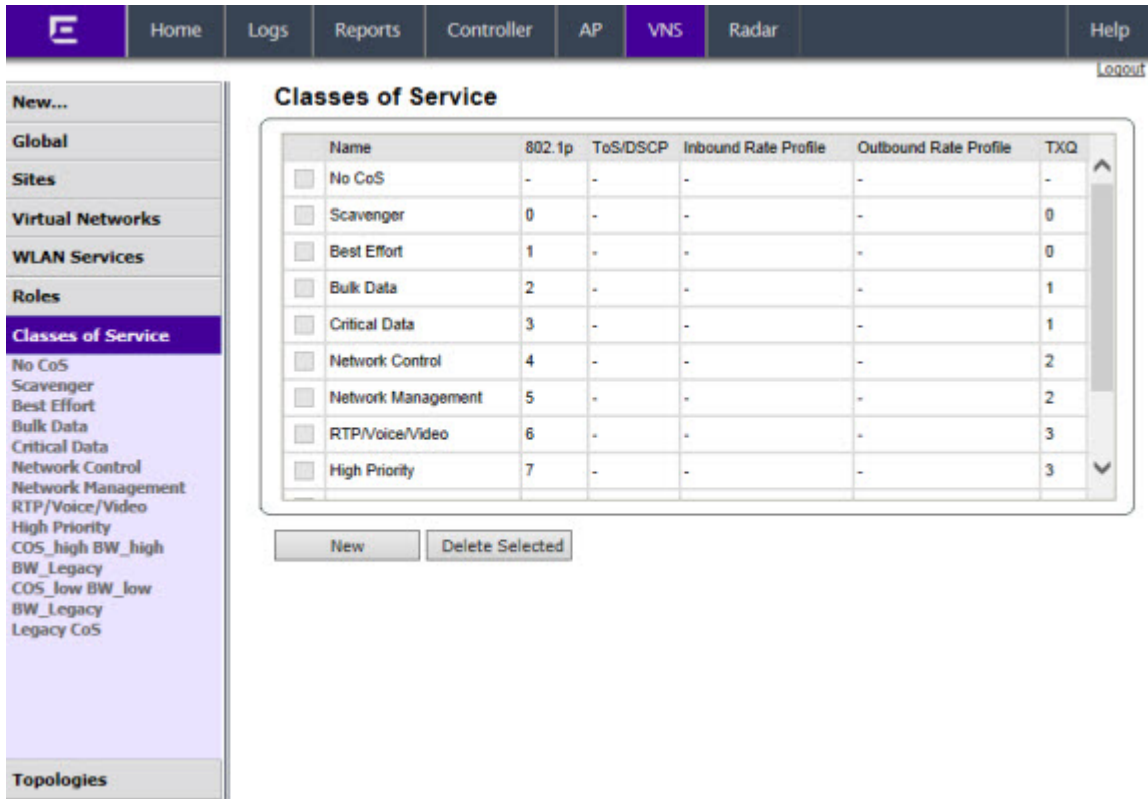
The Classes of Service (CoS) feature is a configuration entity containing QoS Marking (802.1p and ToS/DSCP), Inbound/Outbound Rate Limiting and Transmit Queue Assignments. The CoS ToS marking capability allows for NAC-based redirection to different captive portals on the same WLAN Service.

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**.
The Virtual Network Configuration screen displays.

- 2 In the left pane click Classes of Service. The **Classes of Service** screen displays.



The screenshot shows the 'Classes of Service' configuration page. The left sidebar has 'Classes of Service' selected. The main area displays a table with the following data:

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

Below the table are buttons for 'New' and 'Delete Selected'.

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.

- 3 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 106: General Tab - Fields and Buttons](#) on page 381 describes the fields and buttons on the General tab.

Table 106: 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 283.
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 383. Note: This selection is not available if Legacy Priority Override is checked.

Table 106: 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 383. 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 384.
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 384.
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 CoS 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 CoS 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 Click **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 Click Diffserv Codepoint (DSCP):
 - a Select a Well-known Value or
 - b Enter a Raw Binary Value.
- 5 Close the Configuration dialog.

The logic used to find the final User Priority (UP) depends on the CoS, 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 CoS 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 33: Rate Limiter Example](#) on page 385, 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.

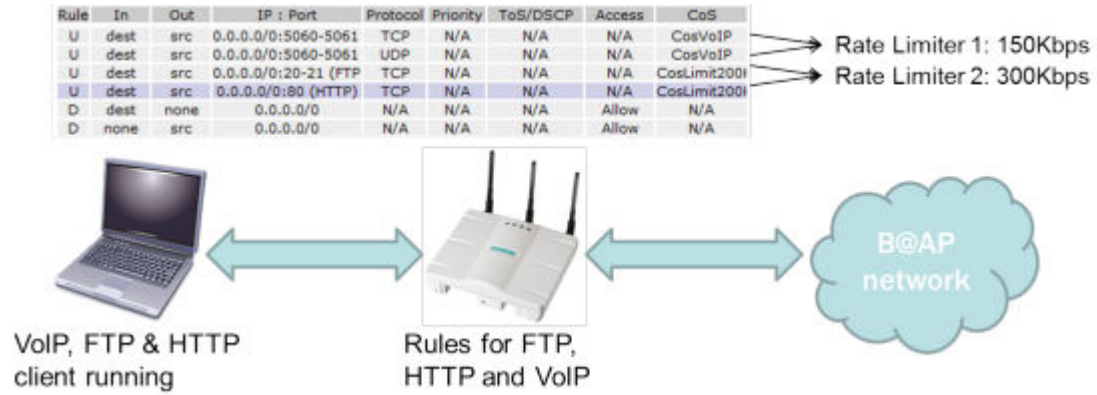


Figure 33: Rate Limiter Example

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, Classes of Service (CoS) 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. Only specific thin series APs (36XX, 37XX, and 38XX) can be applied to a Site, and once an AP is assigned, the controller will preload the APs with 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 170).

Configuring Sites

Topology groups for sites is not support in V9.21. You can add a Role or WLAN to a site, if that Role or WLAN uses a topology group at the time the site is updated. You can also change configuration of a WLAN, Role, and VNS including adding a topology group. Changes to WLAN, Role, and VNS may invalidate the Site configuration. You should change the Role to satisfy requirements for your specific 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, CoS 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 which has local RADIUS client services enabled will use its own RADIUS client to:

- 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.

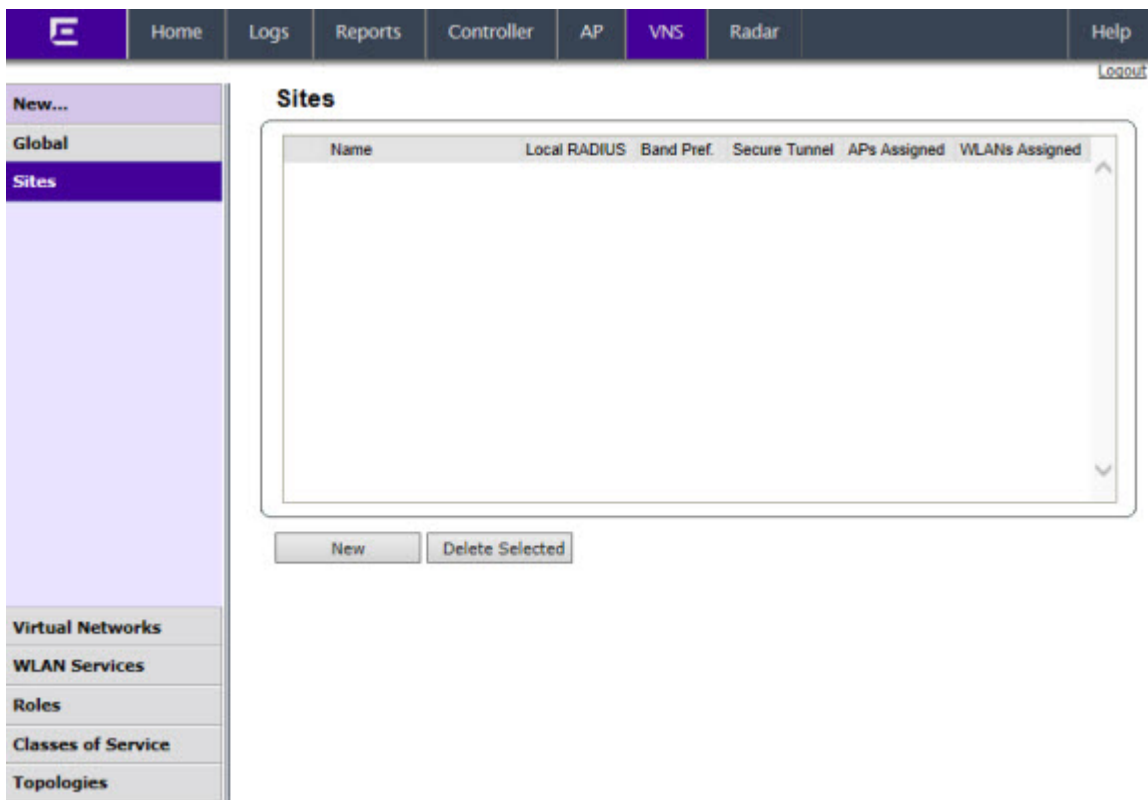
The following guidelines are recommended to configure a secure and easy-to-maintain Site:

- 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**. The **Virtual Network Configuration** screen displays.

- In the left pane, click **Sites**. The **Sites** screen displays.



- 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 107:](#)

Configuration Tab - Fields and Buttons on page 389 describes the fields and buttons on the Configuration tab.

The screenshot shows the 'Site: Configuration' tab in a web interface. The 'Site Name' is 'Temp'. 'Local Radius Authentication' is checked, and the 'Default DNS Server' is '10.10.1.100'. Under 'Roles to download to member APs', 'CNL-422-0-0-default' is selected. The 'RADIUS Servers used' section has a 'Configure...' button. Red text at the bottom states: '- All topologies are downloaded to APs at the site. - DNS server only needs to be configured if RADIUS servers assigned are identified by DNS name'. Buttons for 'Advanced...' and 'Save' are also visible.

Table 107: 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.
CoS 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 391). 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 107: 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 309 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 107: Configuration Tab - Fields and Buttons (continued)

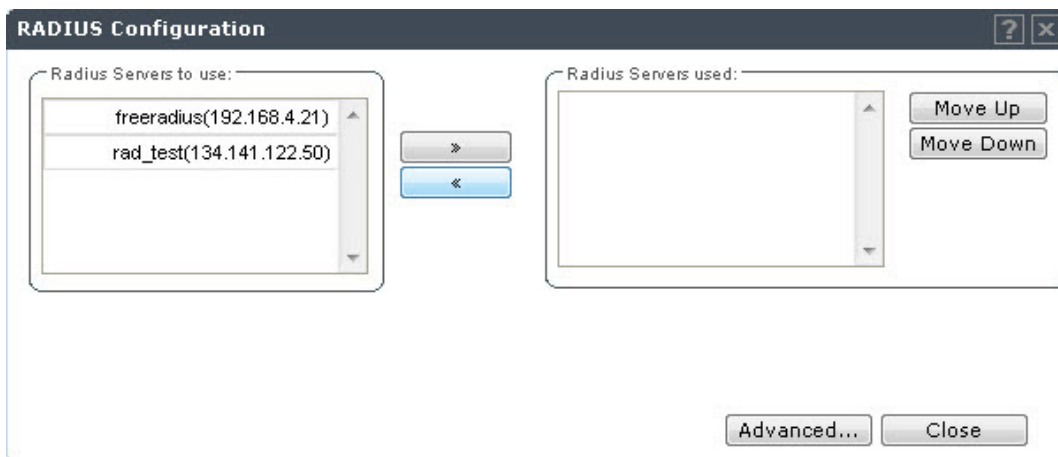
Field/Button	Description
Load Control	<p>Select the following parameters for each radio assigned to this Site:</p> <ul style="list-style-type: none"> • Enable: Select this checkbox to enable Radio Load Control (RLC) for individual radios (Radio1 and Radio2) associated with this Site. • Max. # of Clients: 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
?
✕

NAS IP Address: Use VNS IP address or use:

NAS identifier: Use VNS name or use:

Auth. type: PAP ▼

Password: Unmask

Note: RADIUS Password override is for MBA only

Close

- 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 292) 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:

Click the **AP Assignments** tab. The tab displays, allowing you to select APs that will be applied to this Site configuration.

The screenshot shows a web-based configuration interface for a site. The top navigation bar includes tabs for Home, Logs, Reports, Controller, AP, VNS (selected), Radar, and Help. A 'Logout' link is visible in the top right. On the left, a sidebar menu lists '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	
C4110 - ap2 - AP3620	<input type="checkbox"/>
C4110 - ap3 - AP3825e	<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'. The left sidebar contains a navigation menu with 'Sites' selected. The main content area is titled 'Site:' and has three tabs: 'Configuration', 'AP Assignments', and 'WLAN Assignments'. The 'WLAN Assignments' tab is active, displaying 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



Note

Mesh is supported on all AP36xx models only, excluding the AP3605.

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 Identifi Wireless 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:

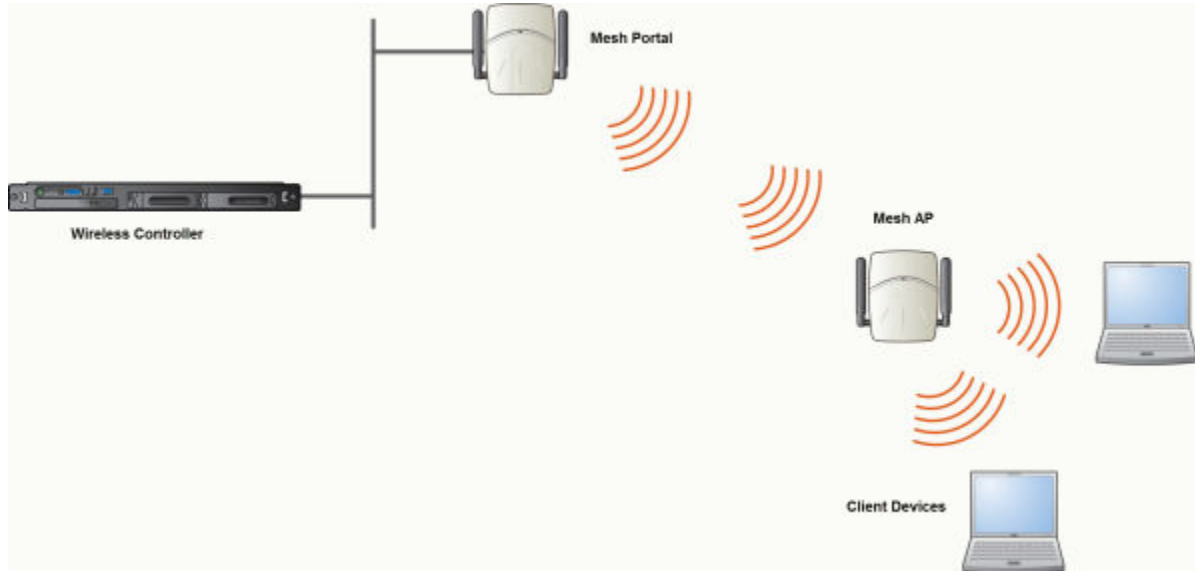


Figure 34: Simple Mesh Configuration

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.

The following figure illustrates the Wireless Repeater configuration:

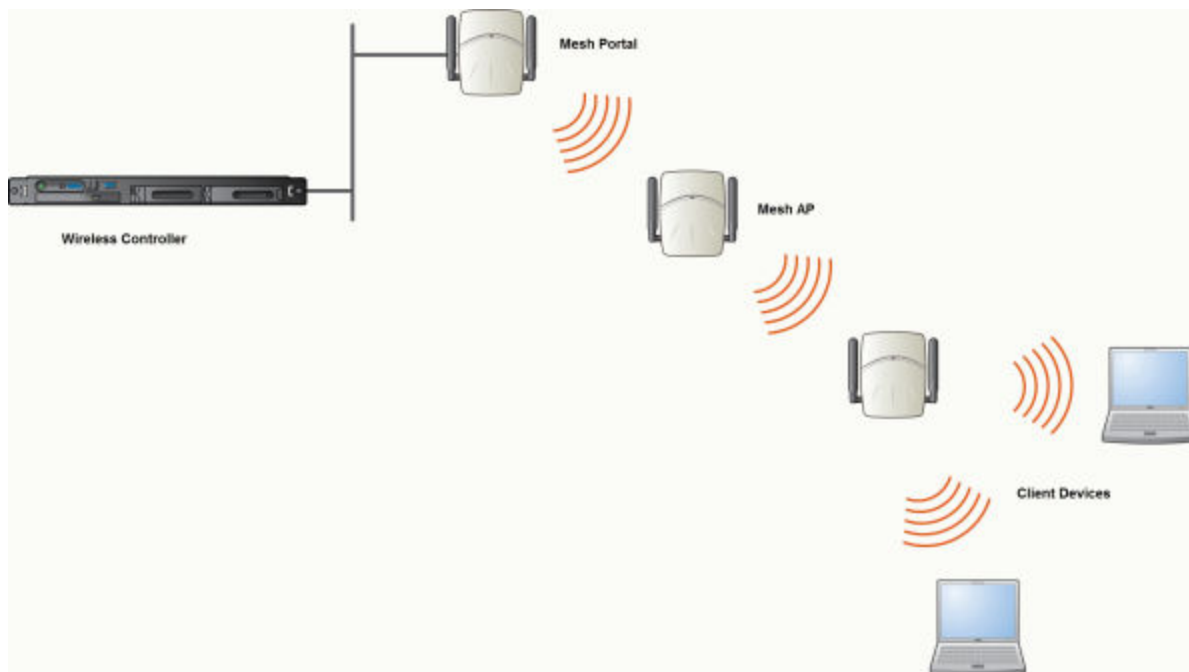


Figure 35: Wireless Repeater Configuration



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.

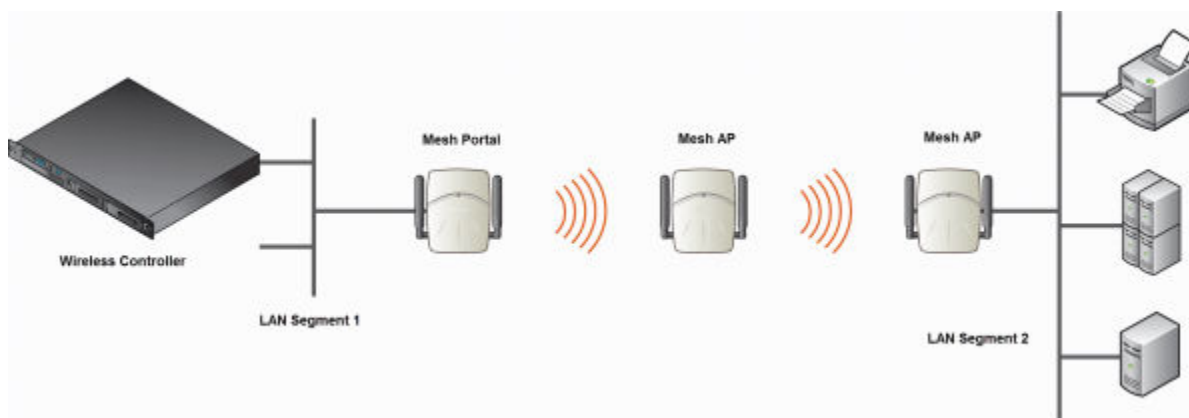


Figure 36: Wireless Bridge Configuration

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.

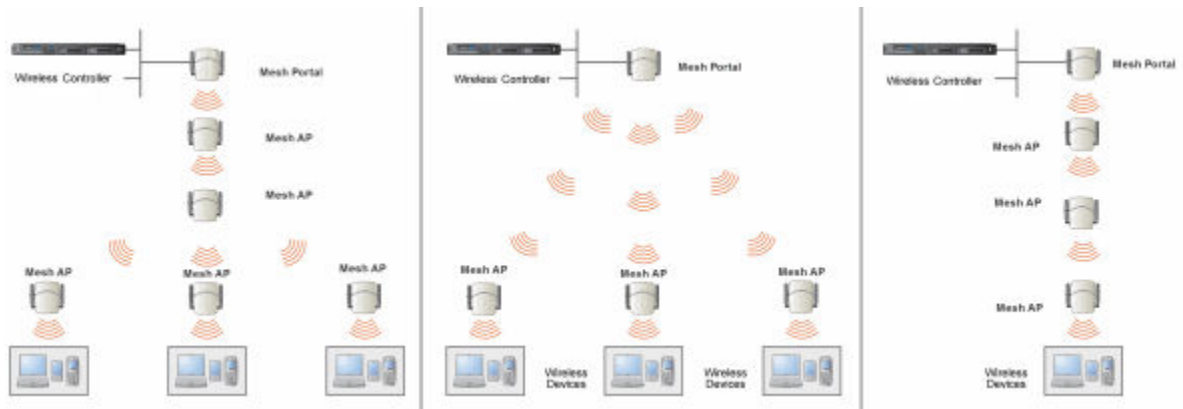


Figure 37: Examples of Mesh Deployment

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 38: Deployment Example](#) on page 399:

- 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.

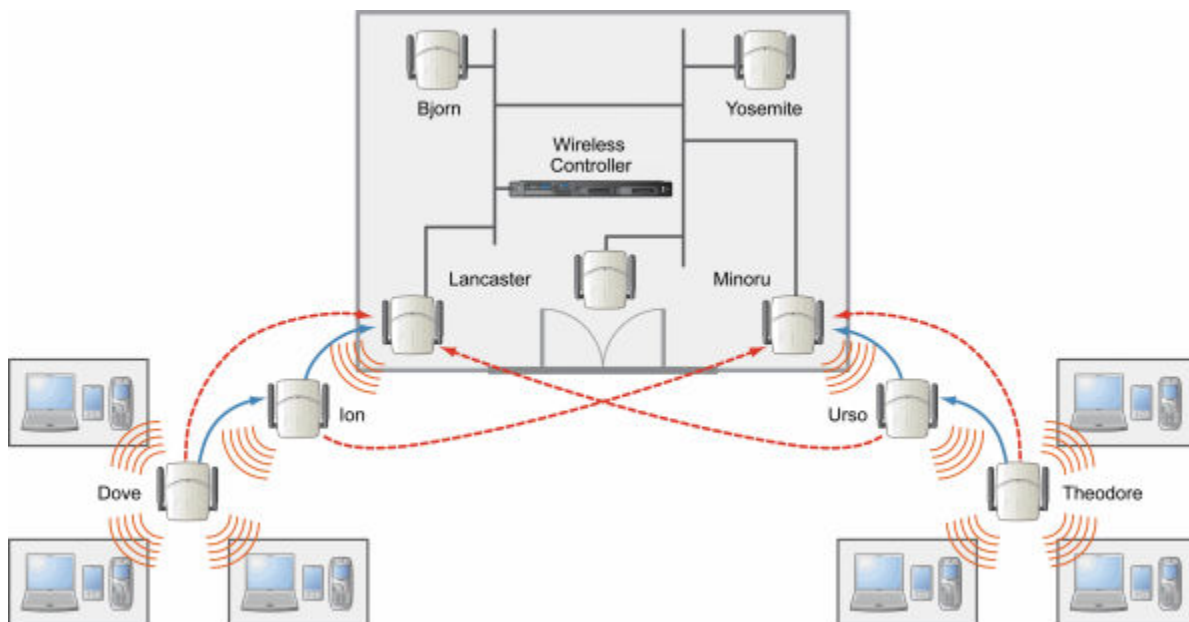


Figure 38: Deployment Example

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 39: Mesh Setup with a Single Mesh WLAN Service](#) on page 400.

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 404.

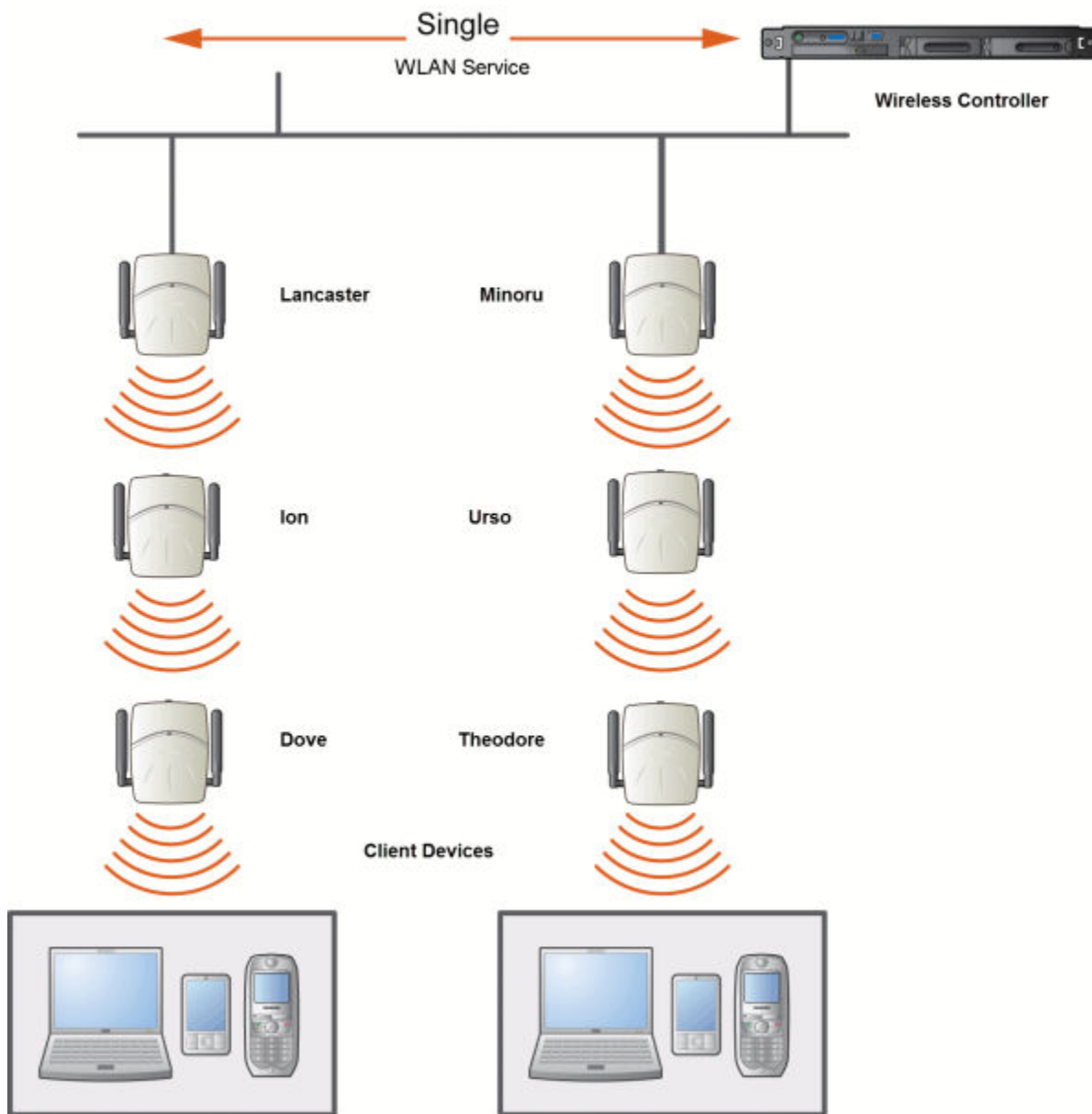


Figure 39: Mesh Setup with a Single Mesh WLAN Service

Mesh Setup with Multiple Mesh WLAN Services

You can also deploy the same Mesh in [Figure 38: Deployment Example](#) on page 399 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.

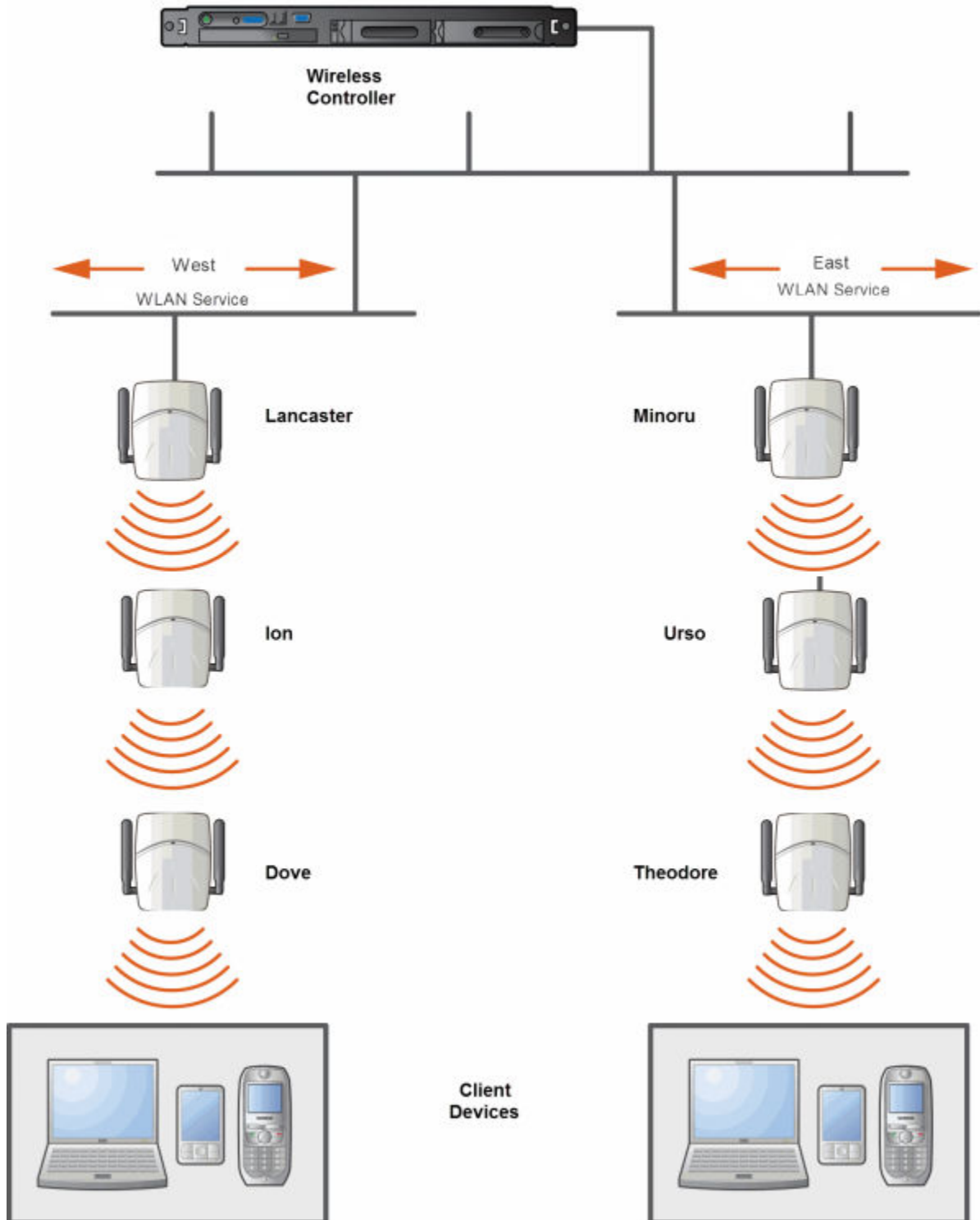


Figure 40: Mesh Setup with Multiple Mesh WLAN Services

Key Features of Mesh

Some key features of Mesh are:

- [Self-Healing Network](#) on page 402
- [Tree-like Topology](#) on page 402
- [Radio Channels](#) on page 403
- [Multi-Root Mesh Topology](#) on page 404
- [Figure 42: Multiple-Root Mesh Topology](#) on page 404

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 41: Parent-Child Relationship Between Wireless APs in Mesh Configuration](#) on page 403 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.

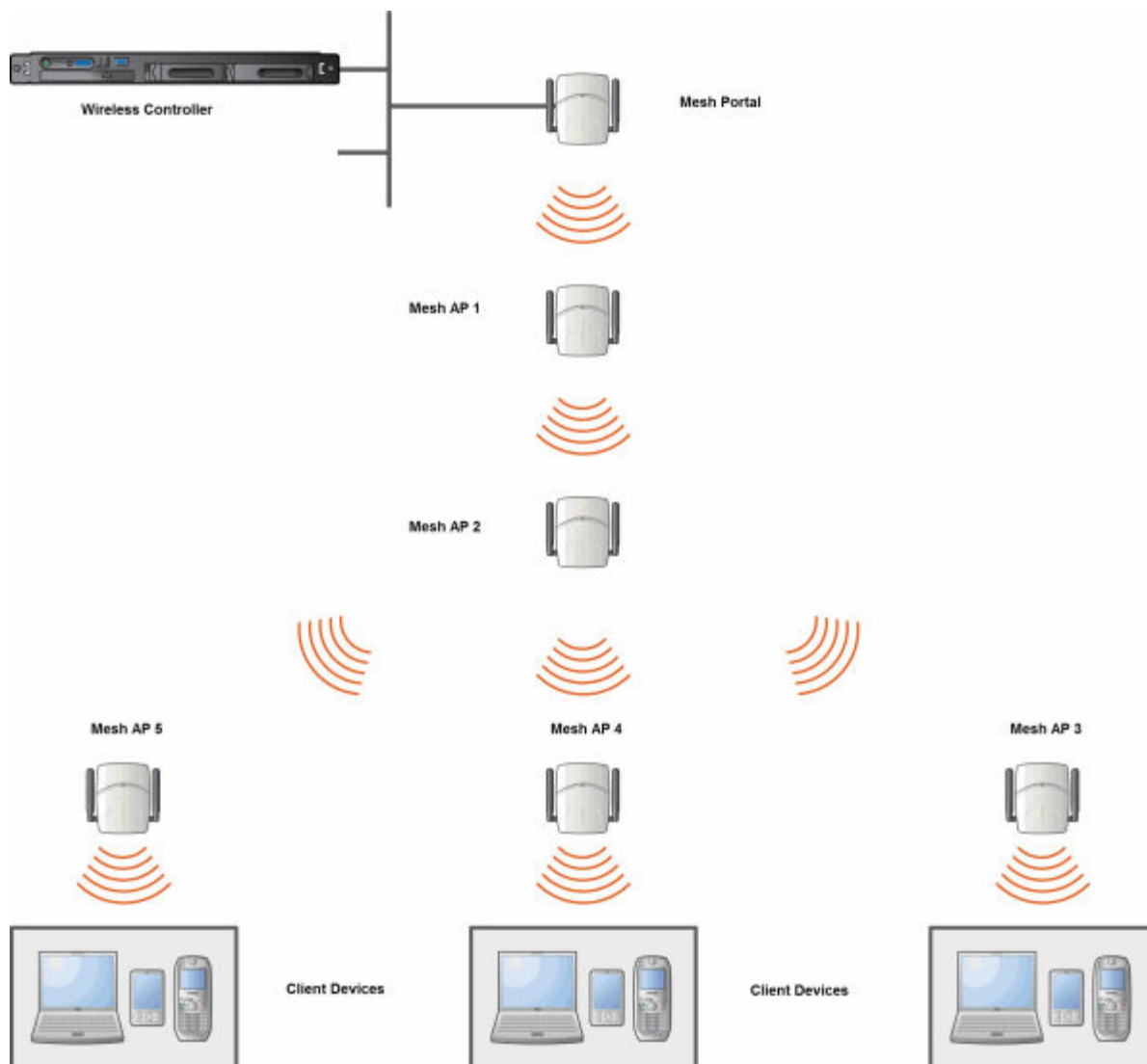


Figure 41: Parent-Child Relationship Between Wireless APs in Mesh Configuration



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 IdentiFi Radar](#) on page 456.



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 42: Multiple-Root Mesh Topology](#) on page 404 illustrates the multiple-root Mesh topology.

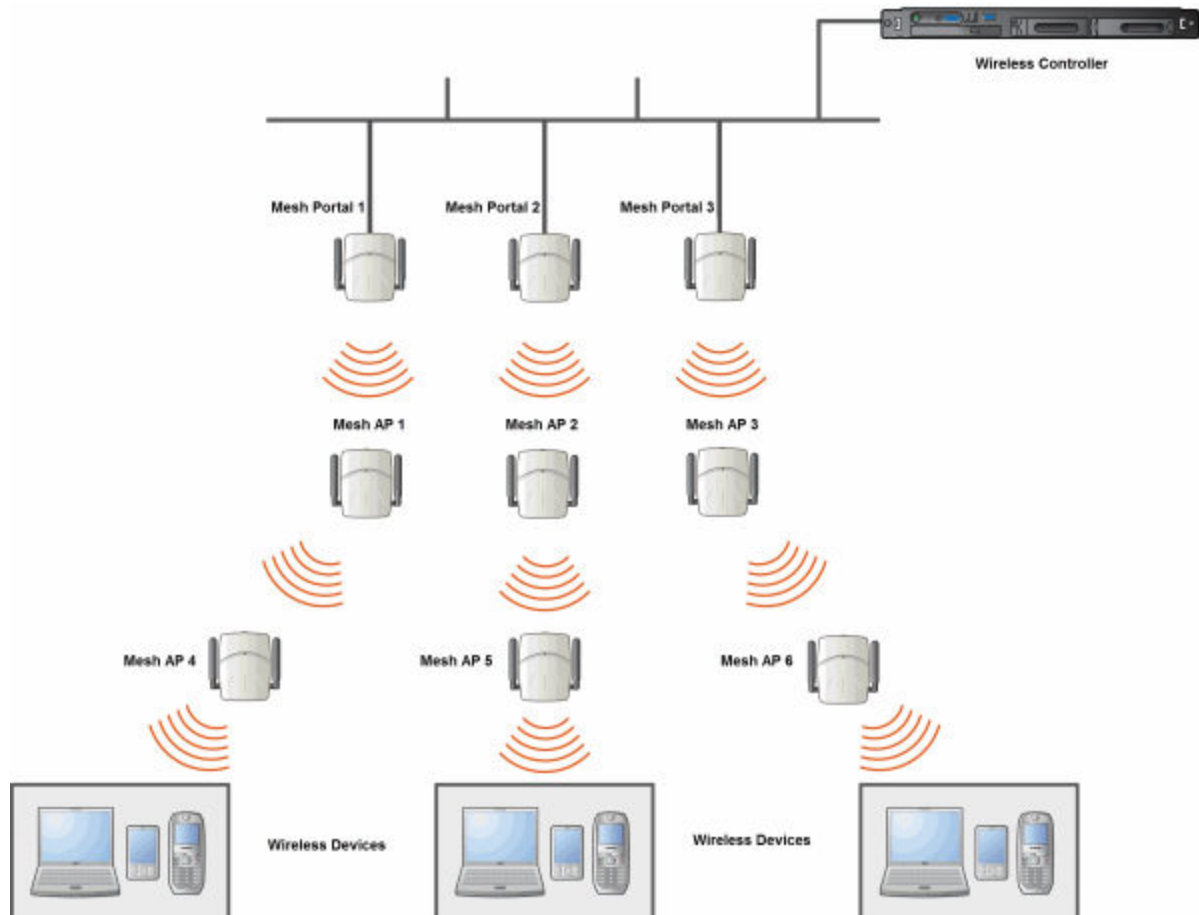


Figure 42: Multiple-Root Mesh Topology

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 Overview](#) on page 112.
- 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 405.
- 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 [Defining Properties for the Discovery Process](#) on page 115. 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 [Manually Adding and Registering a Wireless AP](#) on page 118.

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 43: Mesh Deployment](#) on page 407 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.

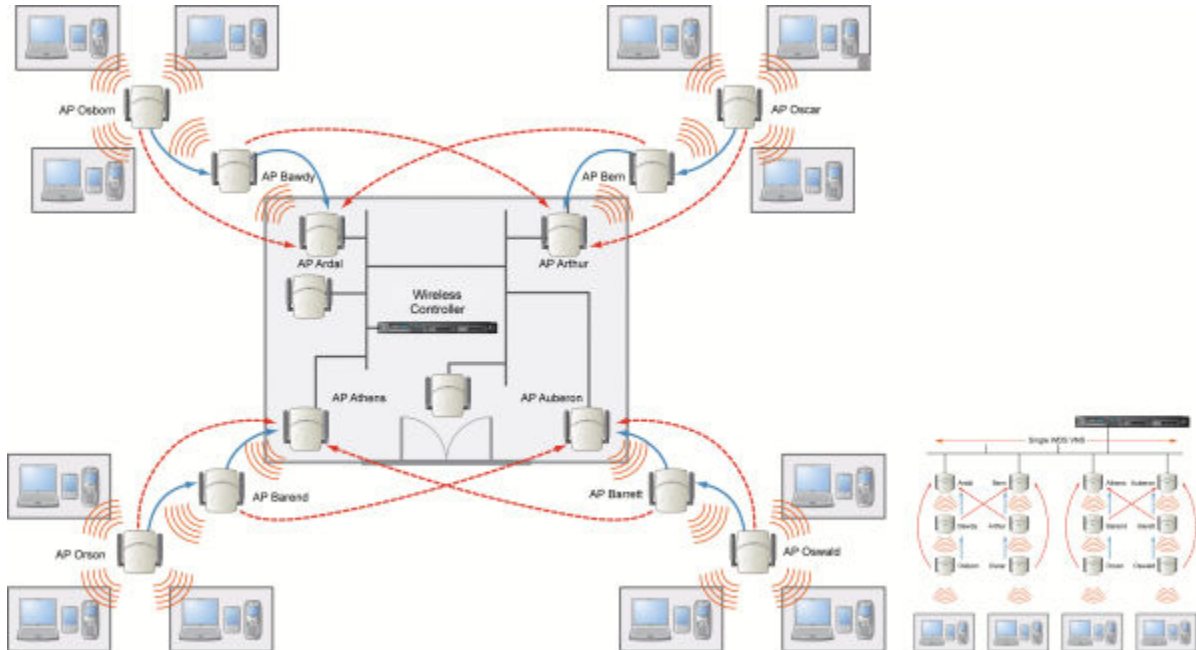


Figure 43: Mesh Deployment

Note



With the single Mesh VNS, the tree structure for the Mesh deployment will be as depicted on the bottom right of [Figure 43: Mesh Deployment](#) on page 407. 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 37: Examples of Mesh Deployment](#) on page 398.

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 VNS (Virtual Network Services) 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 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' text input field, a 'Service Type' section with radio buttons for Standard, WDS, Mesh (selected), Third Party AP, and Remote, and an 'SSID' text input field. Below this is a 'Status' section with an 'Enable' checkbox that 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.

The screenshot shows the 'WLAN: Test' configuration page. The left sidebar contains a navigation menu with categories like Global, Sites, Virtual Networks, WLAN Services (selected), Roles, Classes of Service, and Topologies. The main content area is titled 'WLAN Services' and includes the following fields:

- Core:** Name: Test, Service Type: Mesh, SSID: 10.10.12.1
- Mesh Settings:** Pre-shared Key: (empty), Backhaul Radio: a (5 GHz)
- Status:** Enable:

Below these fields is a table for 'Wireless APs services':

AP Name	Mesh Service	Bridge to LAN	Radio #
C4110 - ap2 - AP3620	none	<input type="checkbox"/>	1
C4110 - ap3 - AP3825e	none	<input type="checkbox"/>	1

A red warning message at the bottom of the table states: "Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot." At the bottom of the page are 'New', 'Delete', and 'Save' buttons.

- 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 410.

- 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 397.

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 405.



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, Changing the radio's Tx Power of a radio on which the Mesh link is established, 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 505.
- 5 Delete the old Mesh WLAN Service. For more information, see [Deleting a VNS](#) on page 378.

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.



Note

All Wireless APs support WDS except for the AP2605, and AP3605.

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:

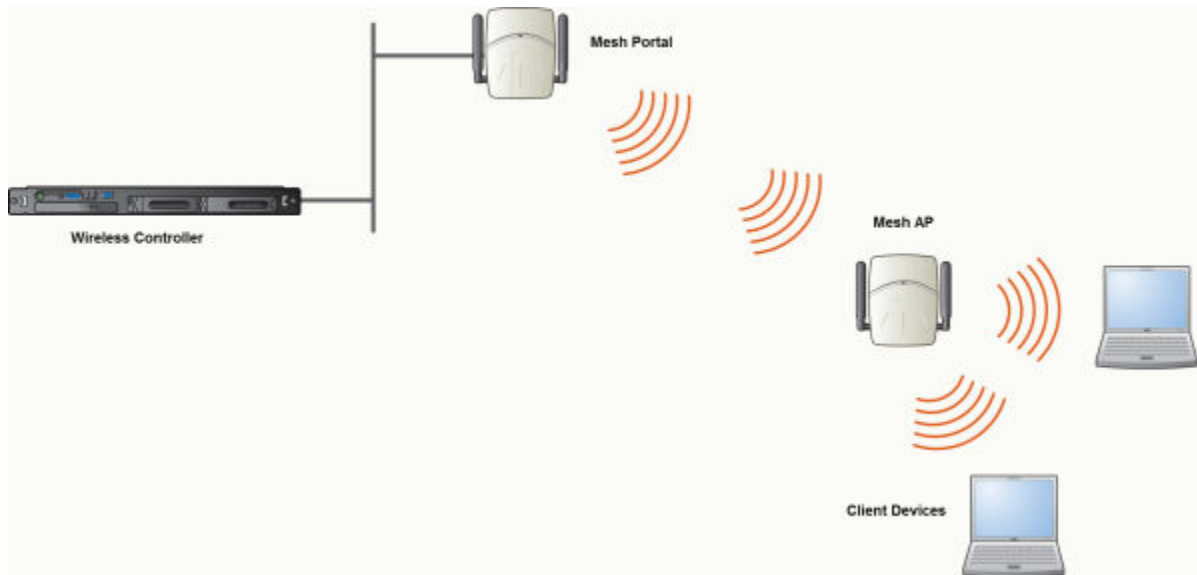


Figure 44: Simple WDS Configuration

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:

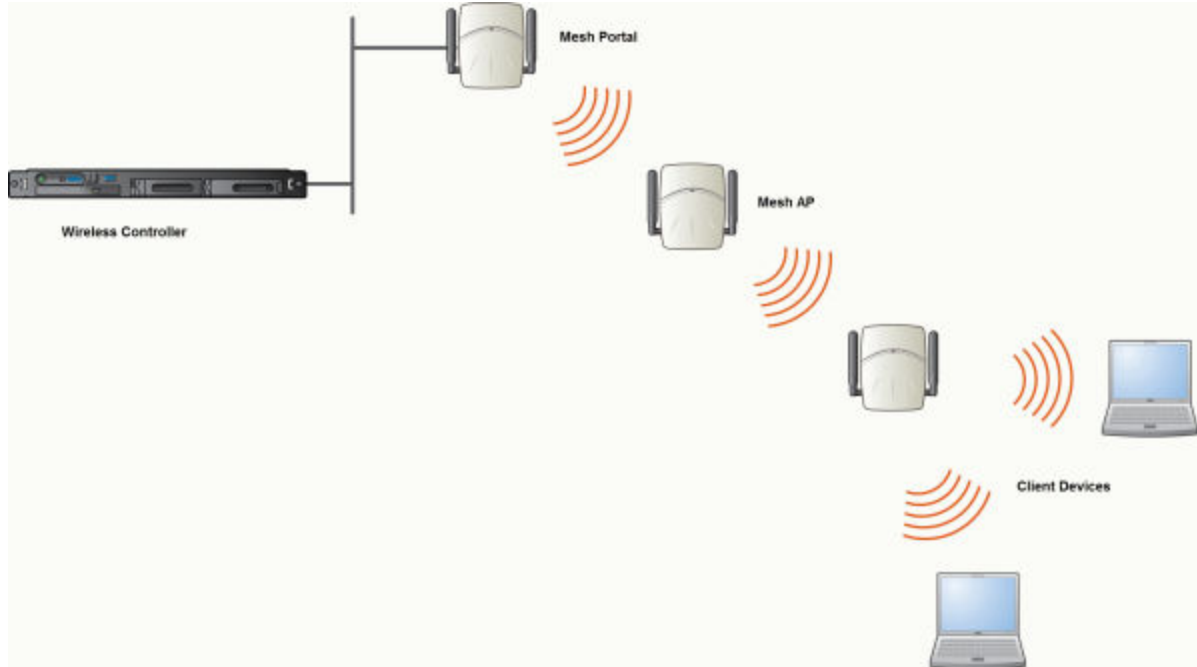


Figure 45: Wireless Repeater Configuration



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.

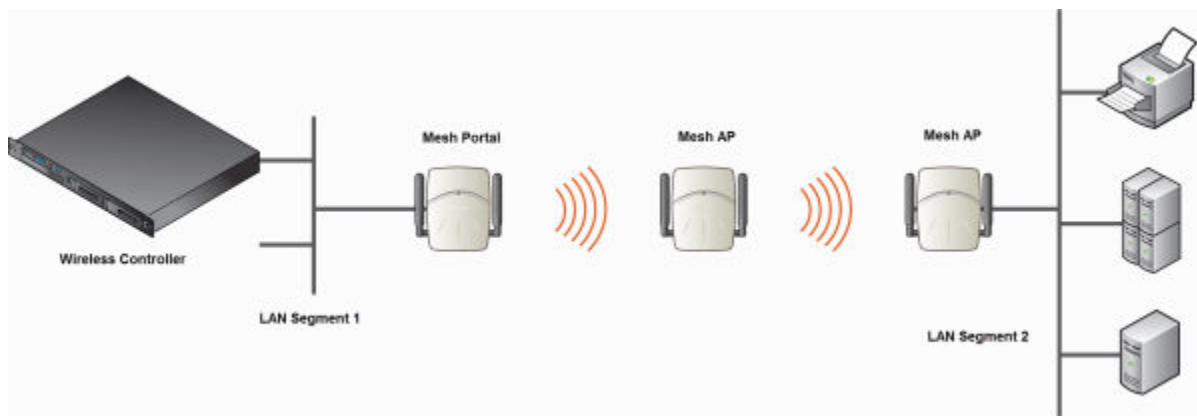


Figure 46: Wireless Bridge Configuration

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.

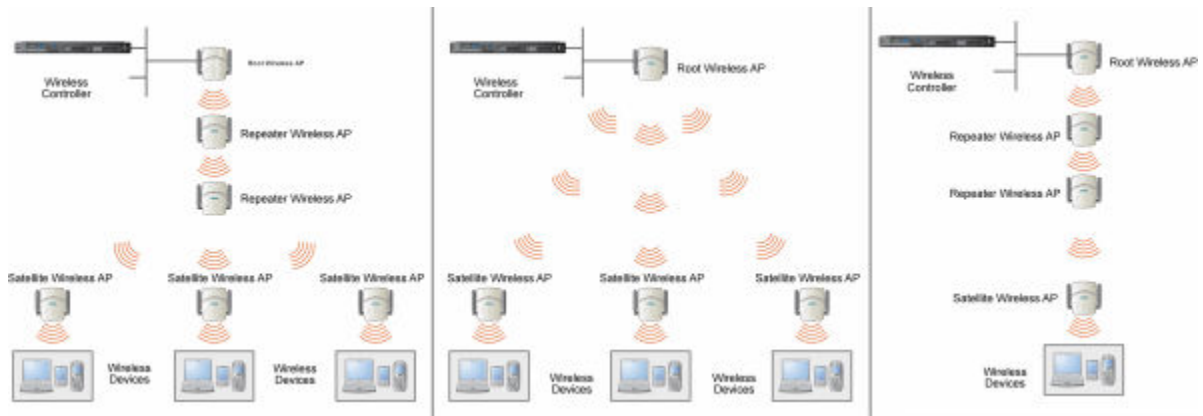


Figure 47: Examples of WDS Deployment

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 427.

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 48: [Deployment Example](#) on page 415 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.

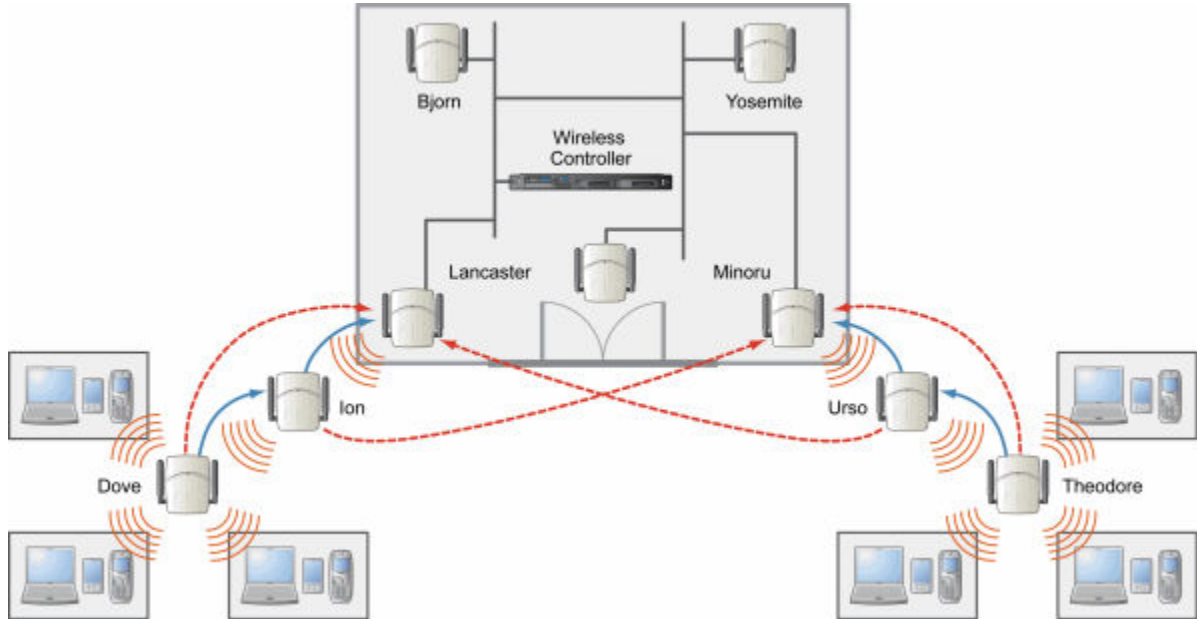


Figure 48: Deployment Example

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 420.

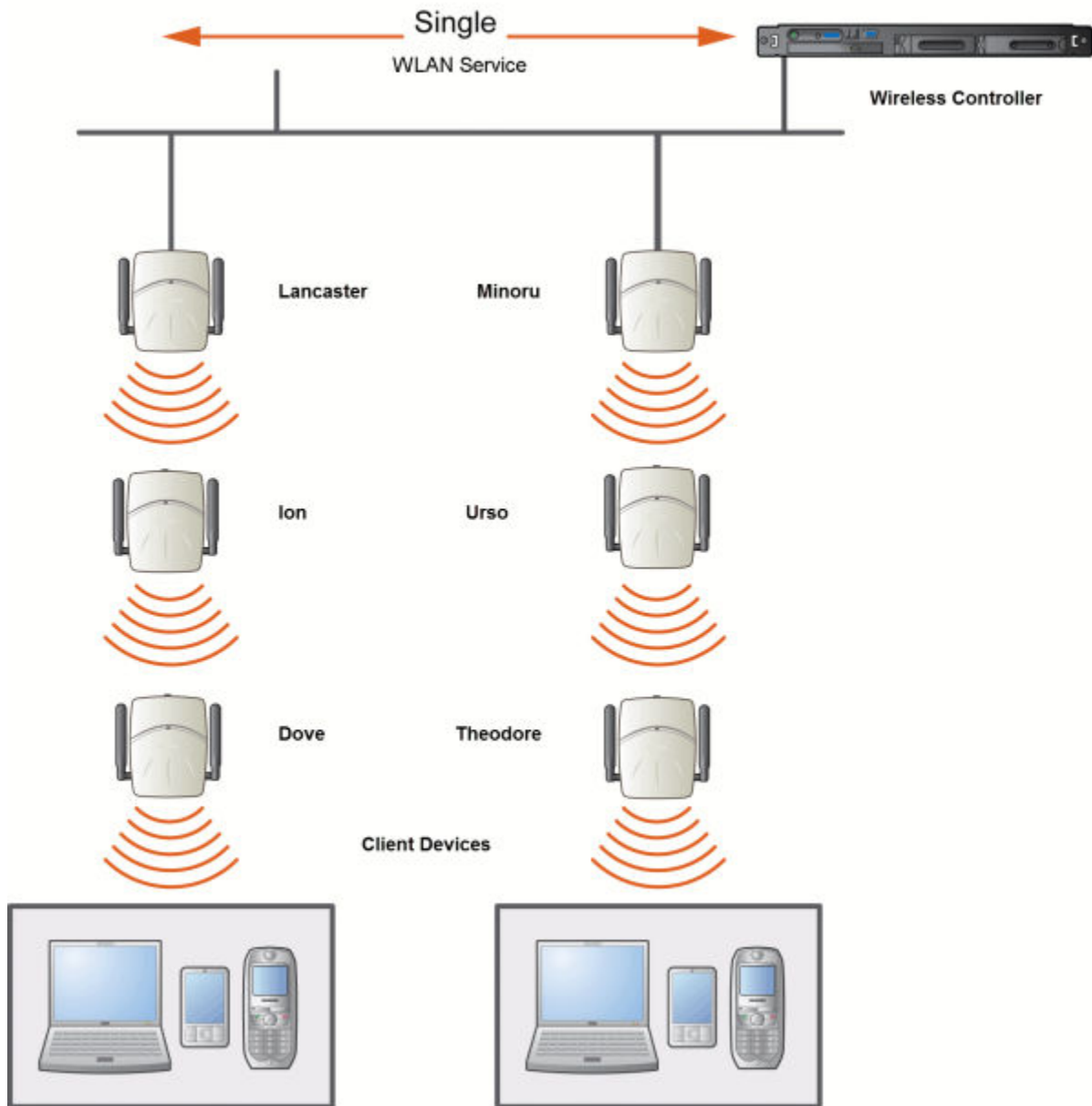


Figure 49: WDS Setup with a Single WDS WLAN Service

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.

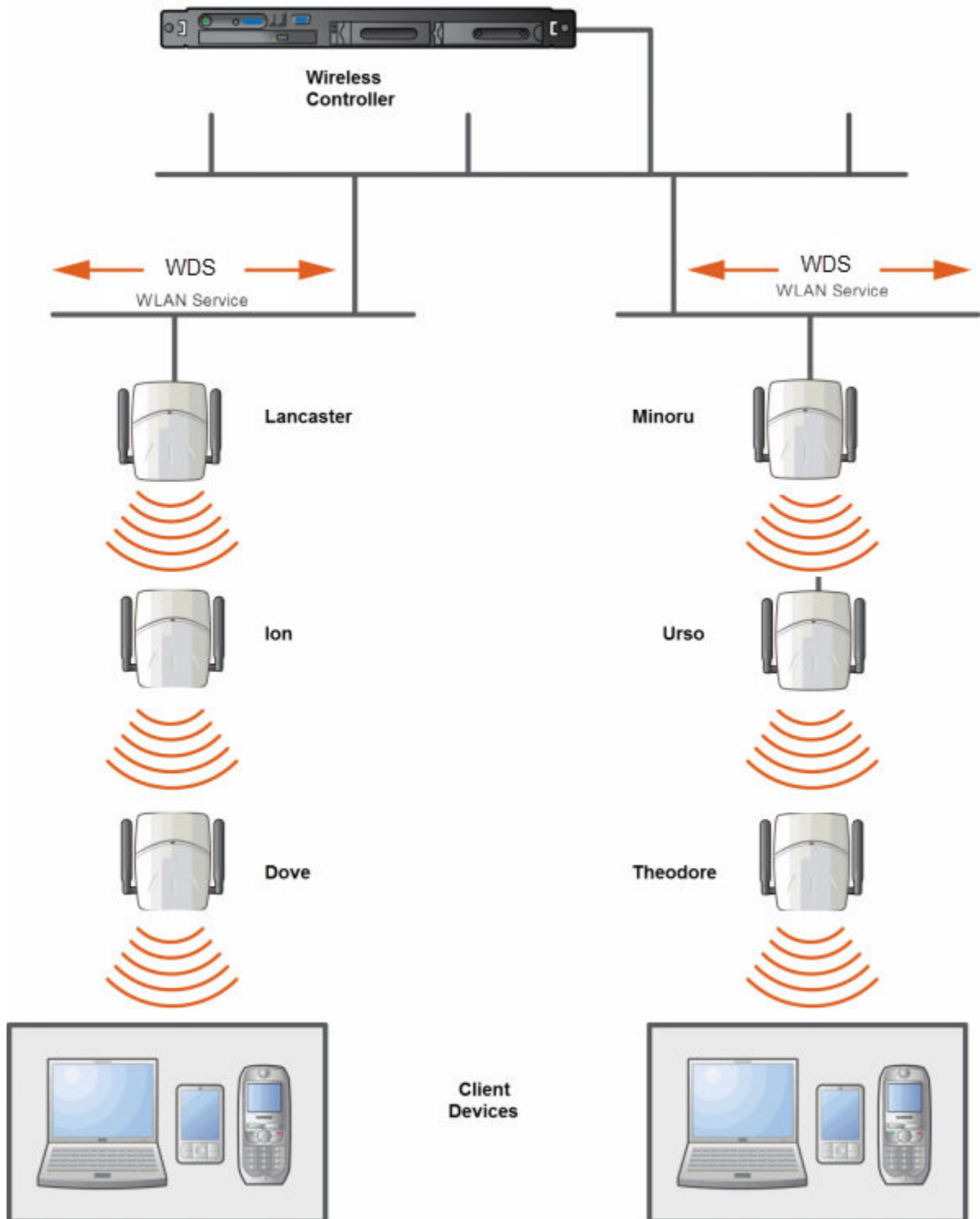


Figure 50: WDS Setup with Multiple WDS WLAN Services

Key Features of WDS

Some key features of WDS are:

- [Tree-like Topology](#) on page 418
- [Radio Channels](#) on page 420
- [Multi-Root WDS Topology](#) on page 420
- [Figure 52: Multiple-root WDS Topology](#) on page 420
- [Link Security](#) on page 421

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 51: Parent-Child Relationship Between Wireless APs in WDS Configuration](#) on page 419:

- 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.

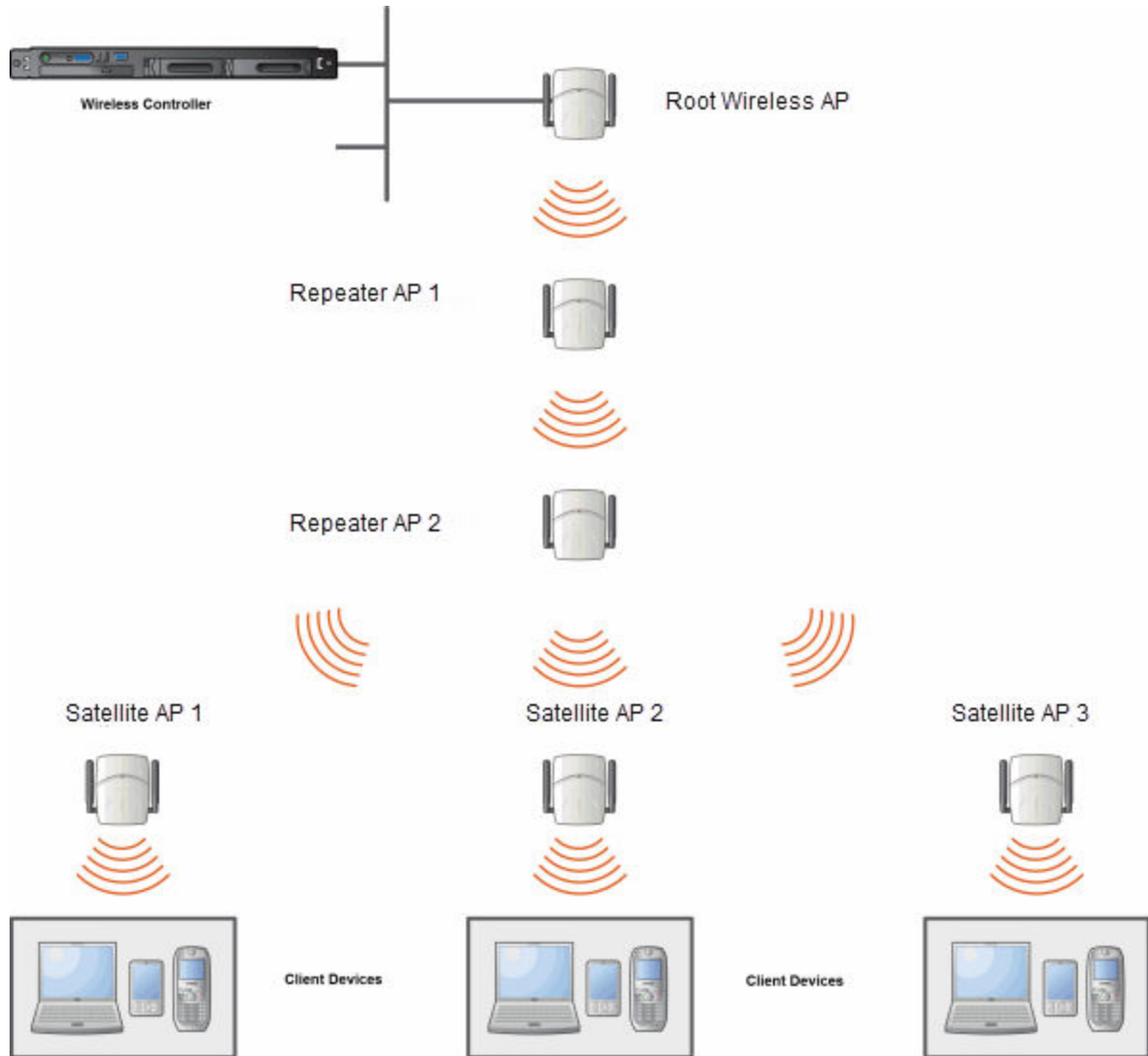


Figure 51: Parent-Child Relationship Between Wireless APs in WDS Configuration

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 IdentifiFi Radar](#) on page 456.

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 52: Multiple-root WDS Topology](#) on page 420 illustrates the multiple-root WDS topology.

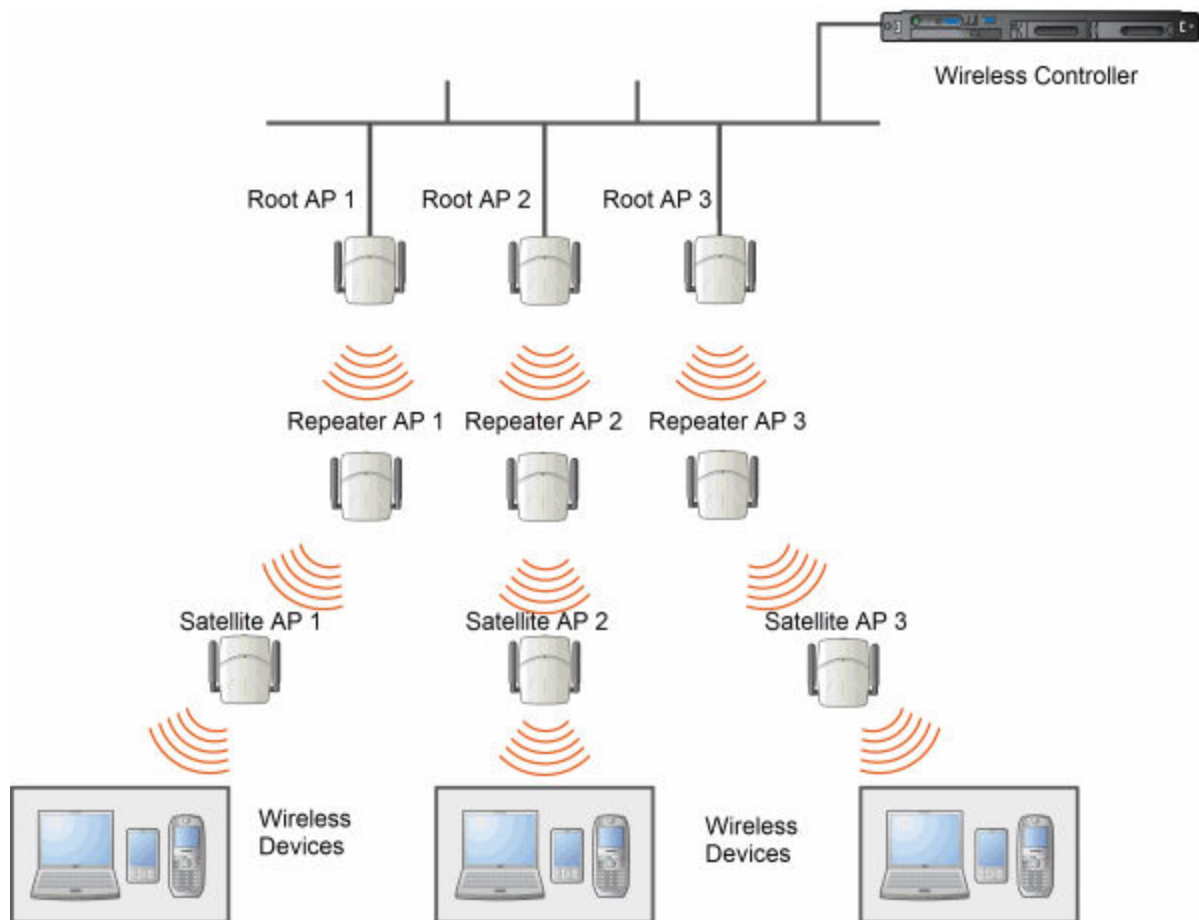


Figure 52: Multiple-root WDS Topology

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 AP's parents and children

Provisioning the WDS Identifi Wireless 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 Overview](#) on page 112.
- 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 IdentifiFi Wireless APs](#) on page 421.
- 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 [Defining Properties for the Discovery Process](#) on page 115. 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 [Manually Adding and Registering a Wireless AP](#) on page 118.

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

Configuring the WDS wireless APs involves the following steps:

- 1 Creating a WDS WLAN Service.
- 2 Defining the SSID name and the pre-shared key.
- 3 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.

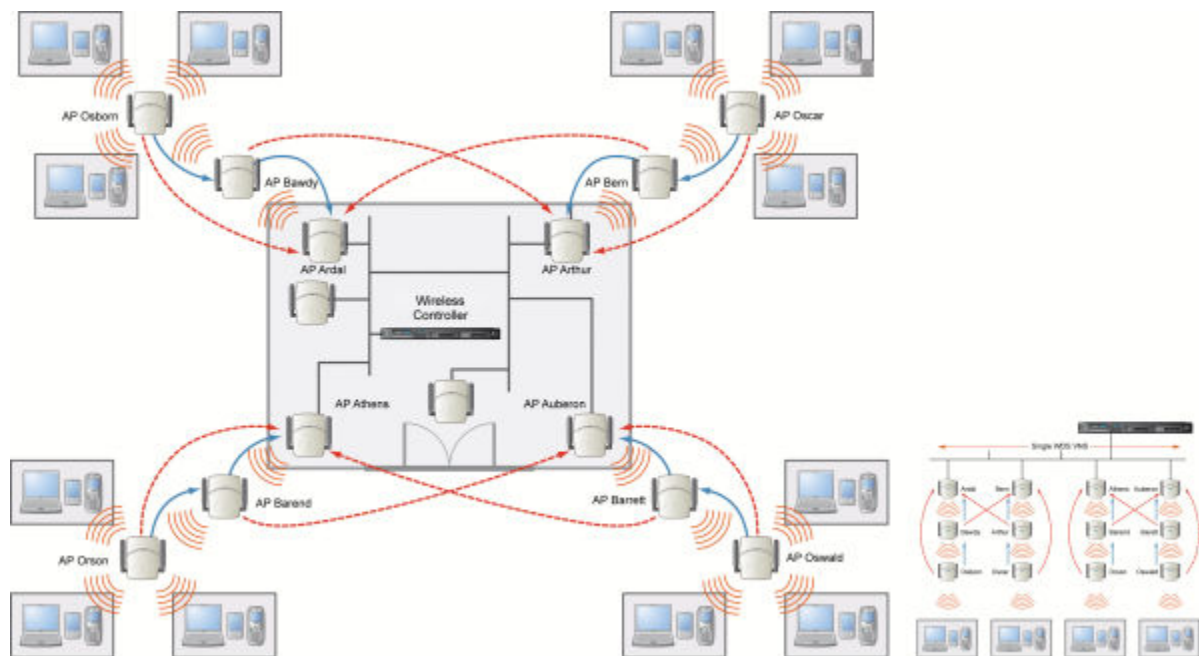


Figure 53: WDS Deployment

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 47: Examples of WDS Deployment](#) on page 414.

To Configure 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.

- 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 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) 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 contains a tree view with categories: New..., Global, Sites, Virtual Networks, and WLAN Services (highlighted). 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 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: WDS

SSID:

WDS Pre-shared key:

Status

Enable:

Wireless APs services

AP Name	Radio 1	Mode	Radio 2	Mode	Preferred Parent
C4110 - ap1 - AP4102	none	a	none	b/g	
C4110 - ap2 - AP3620	none	a/n	none	b/g/n	
C4110 - ap3 - AP3825e	none	a/n/ac	none	b/g/n	

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

New Delete Save

- 7 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 429.

- 8 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.

To configure the WDS with a single WDS VNS, you must assign the roles, preferred parents and backup parents to the APs according to [Table 108: Wireless APs and Their Roles](#) on page 426.

Table 108: Wireless APs and Their Roles

IdentiFi Wireless 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 413.

To assign the roles, preferred parent and backup parent:

- From the radio **b/g** drop-down list of the Root APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
- From the radio **a** drop-down list of the Root APs — Ardal, Arthur, Athens and Auberon, click **Parent**.
- From the radio **a** and radio **b/g** drop-down list of other APs, click the roles according to [Table 108: Wireless APs and Their Roles](#) on page 426.

- d From the **Preferred Parent** drop-down list of other APs, click the parents according to [Table 108: Wireless APs and Their Roles](#) on page 426.
- e From the **Backup Parent** drop-down list of other APs, click the backup parents according to [Table 108: Wireless APs and Their Roles](#) on page 426.

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		

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

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 292.

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 IdentifiFi Wireless APs](#) on page 421.

**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, Changing the radio's Tx Power of a radio on which the WDS link is established, 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 505.
- 4 Delete the old WDS WLAN Service. For more information, see [Deleting a VNS](#) on page 378.

13 Availability and Session Availability

Availability
Session Availability
Viewing SLP Activity

Availability

The Extreme Networks IdentifiFi Wireless 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 119.

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 438.

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 DHCP 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 **IdentiFi Wireless Appliance > Availability** screen. For more information, see [AP Properties Tab Configuration](#) on page 138.

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, you must set the Poll Timeout value for all APs to 15 seconds, and the Detect link failure on the **IdentiFi Wireless Appliance > Availability** screen to ten 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**. The **Controller Configuration** screen displays.
- 2 In the left pane, click **Administration > Availability**. The availability configuration screen displays.

- 3 In the **Availability Wizard** section, click **Start**.
The **Availability Pair Wizard** screen displays.

- 4 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.
- 5 In the **Synchronize Options** section, do the following:

- **Synchronize System Configuration** — Select this checkbox to push the configured **Routed** and **Bridge Traffic Locally at Controller** VNS definitions from the primary controller to the peer controller. **WDS** and **3rd Party AP VNS** definitions are ignored and not synchronized.



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.
- 6 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, DHCP 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** and then **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 315. 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**. The **AP** screen displays.
- 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 136.

- 10 To save your changes, click Save.



Note

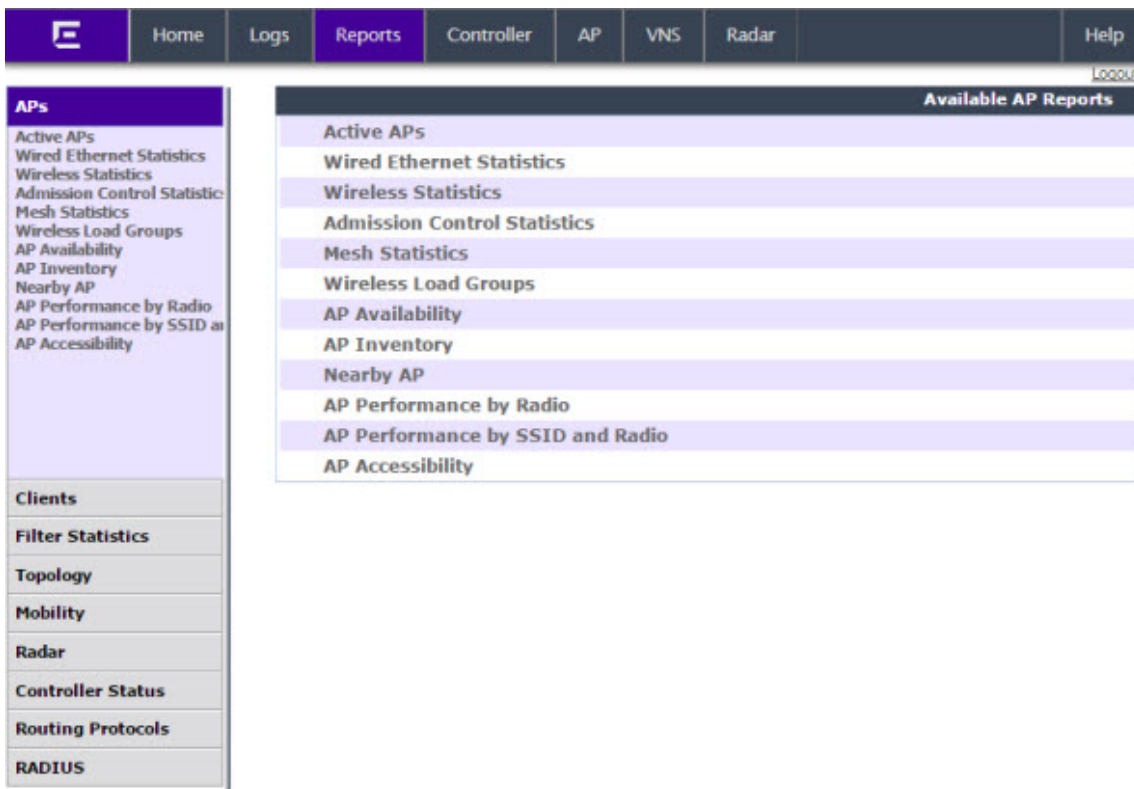
When two controllers have been paired as described above, each controller's registered APs will appear as foreign on the other controller in the list of available APs when configuring a VNS topology.

- 11 Verify that availability is configured correctly.

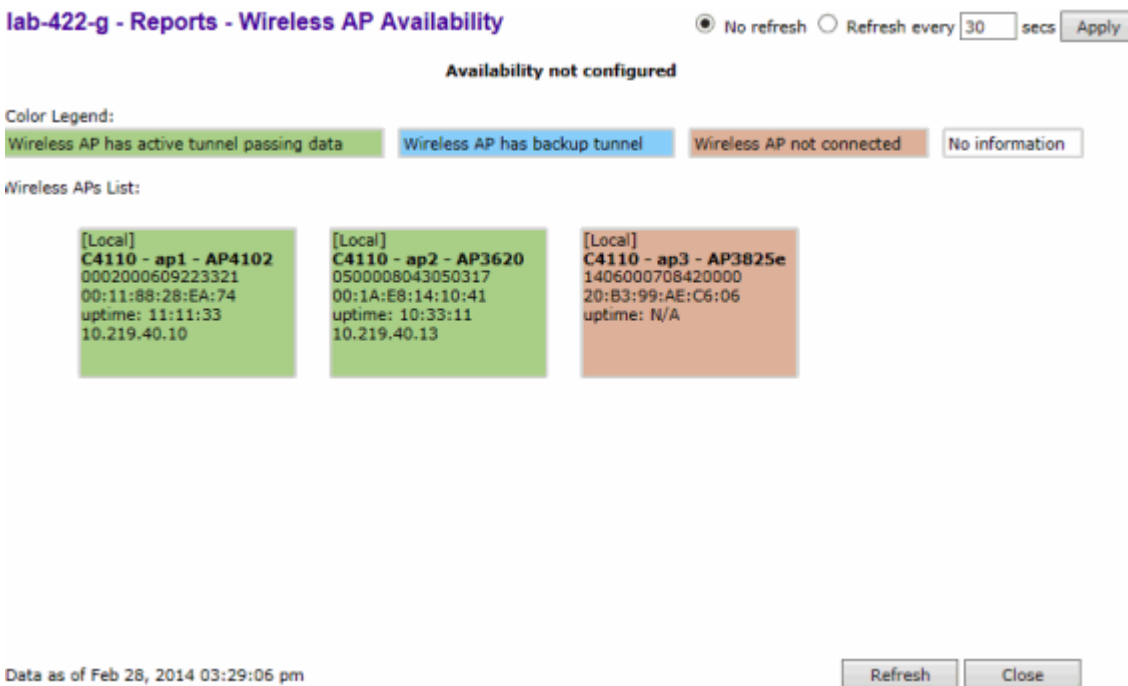
Verifying Availability

To verify that availability is configured correctly:

- 1 From the top menu of either of the two controllers, click **Reports**. The Available AP Reports screen displays.



- 2 From the **Reports and Displays** menu, click **AP Availability**. The Wireless Availability Report is displayed.



- 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 Identifi Wireless *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 goes down ([Figure 54: AP Fail Over to 2ndary Controller When Primary Goes Down](#) on page 438).

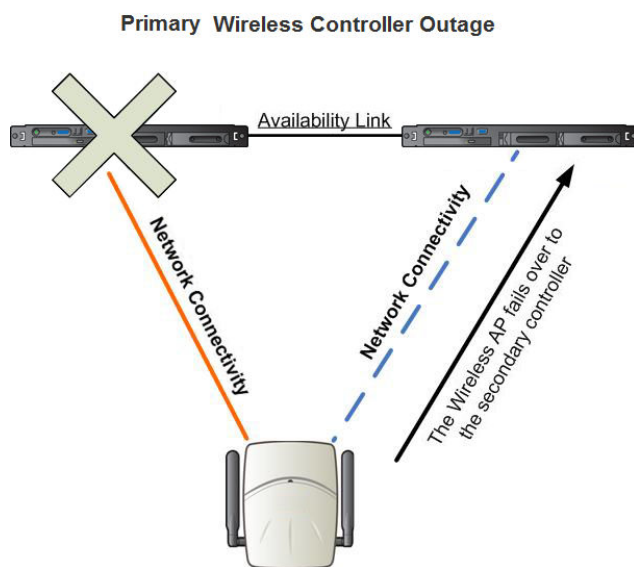


Figure 54: AP Fail Over to 2ndary Controller When Primary Goes Down

- The wireless AP's network connectivity to the primary controller fails ([Figure 55: AP Fail Over to 2ndary Controller When Connectivity to Primary Fails](#) on page 439).

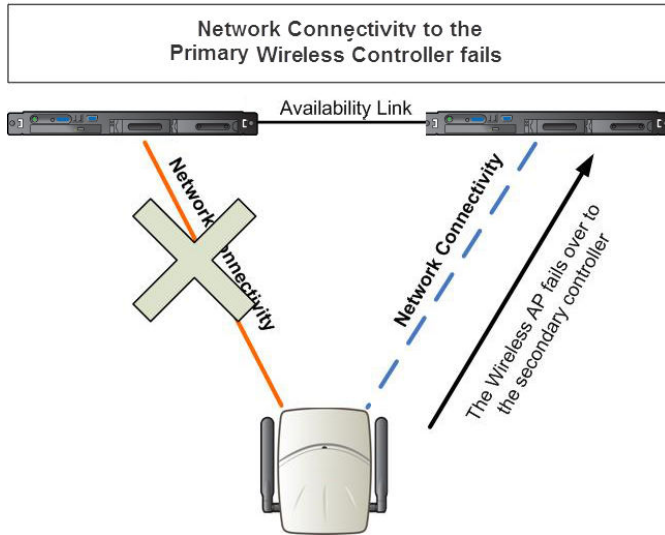


Figure 55: AP Fail Over to 2ndary Controller When Connectivity to Primary Fails

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 56: [Session Availability Mode](#) on page 439), 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.

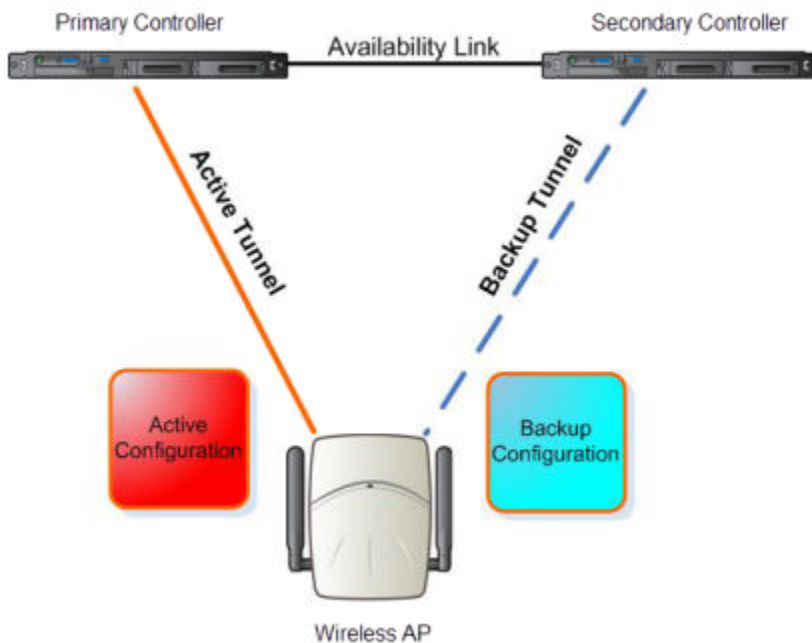


Figure 56: Session Availability Mode

The following is the traffic flow of the topology illustrated in [Figure 56: Session Availability Mode](#) on page 439:

- 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 441.

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 430.
- 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 IdentifiFi Wireless 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 DHCP 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 91.



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**. The **Wireless Controller Configuration** screen displays.
- 3 In the left pane, click **Administration** > **Availability**.

The screenshot shows the 'Availability Wizard' configuration page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar shows 'Administration' with sub-items: 'Availability', 'Flash', 'Host Attributes', 'Installation Wizard', 'Login Management', 'Software Maintenance', 'System Maintenance', and 'Web Settings'. Below the sidebar are sections for 'Logs', 'Network', and 'Services'. The main content area is titled 'Availability Wizard' and contains a 'Start' button. Under 'Controller Availability Settings', the 'Paired' radio button is selected. The 'Wireless Controller IP Address' is set to '0.0.0.0'. There are checkboxes for 'Current Wireless Controller is primary connection point' and 'Fast Failover'. The 'Detect link failure in:' field is set to '8' seconds. Under 'Synchronization Option', both 'Synchronize System Configuration' and 'Synchronize Guest Portal Accounts' are checked. A 'Save' button is located at the bottom right.

- 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 309.

- 8 Click **Save**.
- 9 Set the APs' **Poll Timeout** value for fast failover.
- From the top menu of the primary Controller, click **AP**. The **AP Properties** screen displays.
 - In the left pane, click **Bulk Configuration > AP Multi-edit Settings**. The AP Multi-edit screen displays.

The screenshot shows the 'AP Properties' configuration page. The left sidebar has 'Bulk Configuration' selected, with 'AP Multi-edit Settings' also visible. The main content area is titled 'AP Properties [Hide]' and contains several configuration fields: Location (dropdown), Zone (dropdown), Poll Timeout [Seconds] (text input), Secure Tunnel (dropdown), Secure Tunnel Lifetime [hours] (text input), Remote Access (dropdown), Location-based Services (dropdown), Maintain client sessions in event of poll failure (dropdown), Restart service without controller (dropdown), Use broadcast for disassociation (dropdown), LLDP (dropdown), IP Multicast Assembly (dropdown), LED (dropdown), Country (dropdown), and Antennas (Professional Installer). Below these is the 'Radio Settings [Hide]' section, which includes 'Radio 1' and 'Radio 2' sub-sections, each with an 'Admin Mode' dropdown. At the bottom are 'Reset' and 'Save' buttons.

- In the **Hardware Types** list, select the hardware type of the APs that are part of your deployment. You can select multiple hardware types by pressing the **CTRL** key and clicking the hardware in the **Hardware Types** list.
- In the **Wireless APs** list, select the APs for which you want to set the **Poll Timeout** value. You can select multiple APs by pressing the **CTRL** key and clicking the APs in the **Wireless APs** list.
- In the **Poll Timeout** box, type/edit the appropriate value.
- To save your changes, click **Save**.



Note

The fast failover configuration must be identical on both the primary and secondary controllers. Logs are generated if the configuration is not identical. For more information, see the Extreme Networks *IdentiFi Wireless 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 430.
- The fast failover feature is properly configured. For more information, see [Configuring Fast Failover and Enabling Session Availability](#) on page 441.



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, DHCP and RADIUS servers etc.— is synchronized. For more information, see [Configuring Network Time](#) on page 91.
- 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 **Available AP Reports** screen displays.

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 Identifi Wireless *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:

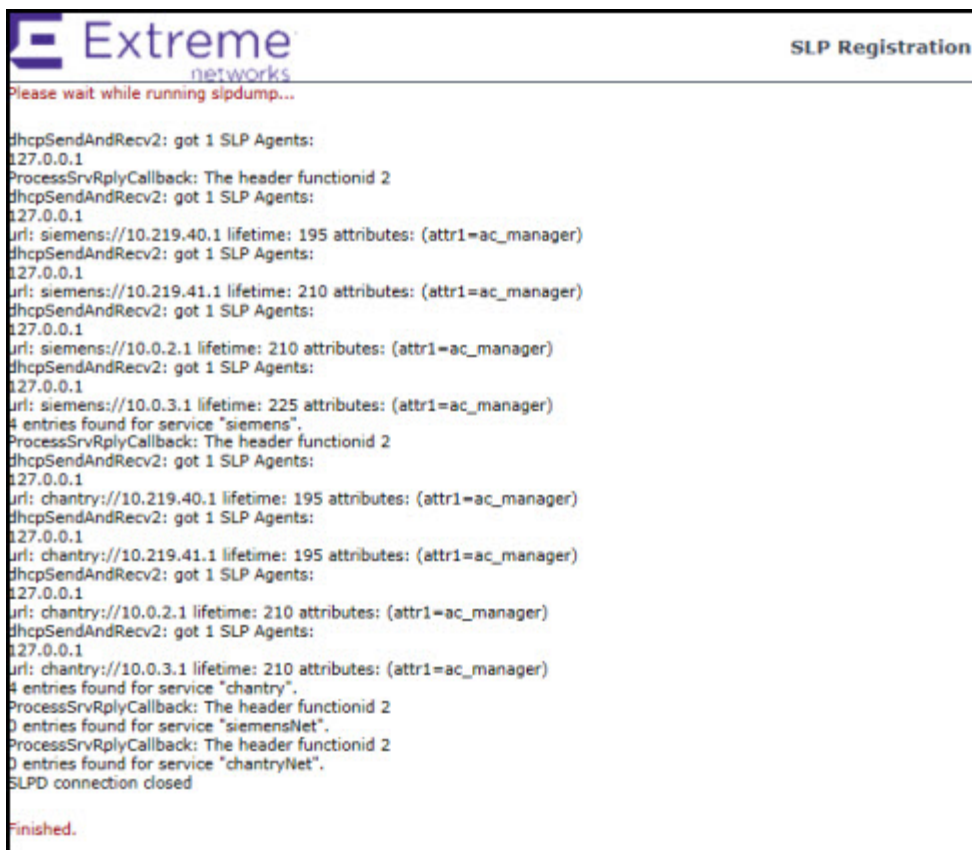
- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Global Settings** > AP Registration. The **Wireless AP Registration** screen displays.

The screenshot shows the 'Wireless AP Registration' configuration page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. A 'Logout' link is visible in the top right corner. The left sidebar contains a tree view with 'Global Settings' selected, and sub-items for 'AP Maintenance', 'AP Registration', and 'WAS Sensor Management'. The main content area is titled 'Wireless AP Registration' and contains the following sections:

- 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)
- Telnet Access:**
 - Password:
 - Confirm password:
- SSH Access:**
 - Password:
 - Confirm password:
- Secure Cluster:**
 - Cluster Shared Secret:
 - Use Cluster Encryption Inter AP Room

At the bottom of the page, there are two buttons: 'View SLP Registration' and 'Save'.

- To confirm SLP registration, click **View SLP Registration**. A screen displays the results of the diagnostic slpdump tool, to confirm SLP registration.



```
Extreme networks SLP Registration
Please wait while running slpdump...

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://10.219.40.1 lifetime: 195 attributes: (attr1=ac_manager)
dhcpSendAndRecv2: got 1 SLP Agents:
127.0.0.1
Url: siemens://10.219.41.1 lifetime: 210 attributes: (attr1=ac_manager)
dhcpSendAndRecv2: got 1 SLP Agents:
127.0.0.1
Url: siemens://10.0.2.1 lifetime: 210 attributes: (attr1=ac_manager)
dhcpSendAndRecv2: got 1 SLP Agents:
127.0.0.1
Url: siemens://10.0.3.1 lifetime: 225 attributes: (attr1=ac_manager)
4 entries found for service "siemens".
ProcessSrvRplyCallback: The header functionid 2
dhcpSendAndRecv2: got 1 SLP Agents:
127.0.0.1
Url: chantry://10.219.40.1 lifetime: 195 attributes: (attr1=ac_manager)
dhcpSendAndRecv2: got 1 SLP Agents:
127.0.0.1
Url: chantry://10.219.41.1 lifetime: 195 attributes: (attr1=ac_manager)
dhcpSendAndRecv2: got 1 SLP Agents:
127.0.0.1
Url: chantry://10.0.2.1 lifetime: 210 attributes: (attr1=ac_manager)
dhcpSendAndRecv2: got 1 SLP Agents:
127.0.0.1
Url: chantry://10.0.3.1 lifetime: 210 attributes: (attr1=ac_manager)
4 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 Extreme Networks IdentifiFi Wireless 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 DHCP 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 will 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 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 any availability
- Mobility domain with availability
- Mobility domain with session availability



Note

If you are configuring mobility, you must synchronize time on all the wireless controllers that are part of the mobility domain. For more information, see [Configuring Network Time](#) on page 91.

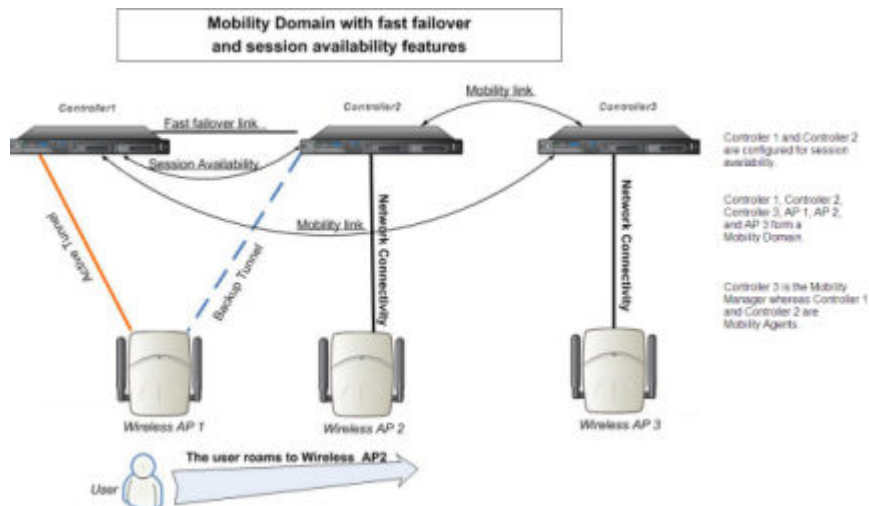


Figure 57: Mobility Domain with Fast Failover and Session Availability Features

- 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.
 - AP 1 establishes active session with Controller 2. AP 2 is not impacted by the failover.

Configuring a Mobility Domain

If you are configuring a mobility domain with availability or session availability, you must synchronize time on all the wireless controllers that are part of your mobility domain. For more information, see [Configuring Network Time](#) on page 91.

Designating a Mobility Manager

To Designate a Mobility Manager:

- 1 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Services > Mobility Manager**. The **Mobility Manager Settings** screen displays.

The screenshot shows the 'Mobility Manager Settings' page. 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', and 'Services' (selected). Under 'Services', 'Location-based Service' and 'Mobility Manager' are listed. The main content area is titled 'Mobility Manager Settings' and contains the following options:

- Mobility**
- This Wireless Controller is a Mobility Manager**
 - Port:
 - Heartbeat: seconds
 - SLP Registration:
 - Permission List: **Agent IP Address (State)**
 - Table with 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**

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

- 3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options are displayed.
- 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

If the mobility domain is configured for fast failover and session availability, you should 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 To save your changes, 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**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Services > Mobility Manager**. The **Mobility Manager Settings** screen displays.
- 3 To enable mobility for this controller, 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' page. The navigation menu on the left includes 'Administration', 'Logs', 'Network', 'Services', 'Location-based Service', and 'Mobility Manager'. The 'Mobility' section is checked, and the radio button for 'This Wireless Controller is a Mobility Agent' is selected. The 'Port' dropdown is set to 'Port1 (10.219.40.1)', and the 'Discovery Method' dropdown is set to 'Static Configuration'. There are empty input boxes for 'Mobility Manager Address' and 'Backup Manager Address'. A 'Save' button is visible at the bottom right.

- 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 support the discovery of Extreme NetworksNET service to attempt 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 To save your changes, click **Save**.

For information about viewing mobility manager displays, see [Viewing Mobility Reports](#) on page 525.

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 270.

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 223.
- 2 Define policy rules that allow access to other services and protocols on the network such as HTTP, FTP, telnet, 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 226.

In addition, modify the following functions on the third-party AP:

- Disable the AP's DHCP 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 IdentifiFi Wireless 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 IdentiFi Radar

- Radar Overview
- Radar Components
- Radar License Requirements
- Radar Scan Profiles
- Viewing Existing Scan Profiles
- Enabling the Analysis and Data Collector Engines
- Adding a New Scan Profile
- Configuring a Legacy Scan Profile
- Configuring an In-Service Scan Profile
- Configuring a Guardian Scan Profile
- Maintaining the Radar Lists of APs
- Configuring the Location Engine
- Working with Radar Reports

Radar Overview

Radar is a set of advanced, intelligent features for managing the wireless environment. Radar includes advanced features for:

- Station 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.

Mitigator functionality has been rolled into Radar's Legacy scan profiles. Legacy scan profiles can be used with W786, AP36xx-based APs, and the AP26xx-based APs. Legacy scan profiles require the AP to stop bridging traffic while it attempts to detect a limited subset of possible threats.

All 37xx, and 38xx series APs can provide WIDS and traffic forwarding functionality, simultaneously. All 37xx, 38xx series APs will, if configured to do so, apply countermeasures to detected wireless intrusions.

The 3710, 3715, 376x, 3825, and 3865 APs can be placed in Guardian mode. In this mode the AP dedicates both radios purely to WIDS-WIPS functions. Guardians are capable of detecting and mitigating attacks on wireless channels that are not being used for traffic forwarding by the authorized network.

Radar Components

The following figure [Figure 58: Radar System Components](#) on page 457 illustrates the major components of Radar.

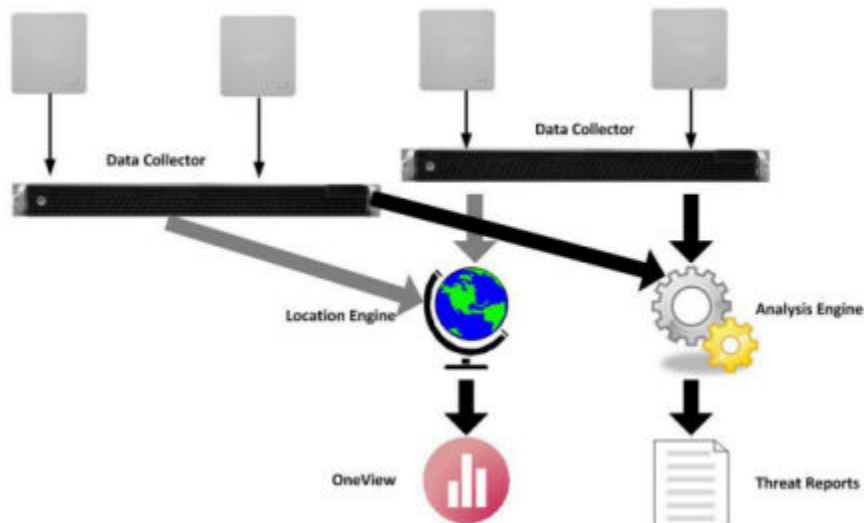


Figure 58: Radar System Components

Analysis Engine Overview

Radar requires that a single controller must be delegated to host the Analysis Engine. A data collector application, installed on each controller, 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, 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, Guardian or Legacy scan profile.

The Analysis Engine relies on a database of connected devices on the Extreme Networks Identifi Wireless 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 and Data Collector Engines](#) on page 462.

Radar Functionality on the Controller

A single Analysis Engine can interact with data collectors on different controllers. The number of different controllers that a single Analysis Engine can work with is a function of the following:

- On all controller models, when at least one In-Service scan profile has been defined for the Analysis Engine, the Analysis Engine can interact with at most 2 controllers, its host and its host's availability partner, if it has one.
- When only Legacy scan profiles are defined, the Analysis Engine on the C4110, C5110, V2110, and C5210 can interact with RF Data Collectors on up to 12 controllers.
- When no In-Service scan profile is defined and at least one Legacy scan profile is defined (created using the old Mitigator engine), the Analysis Engine on the C25 and C35 can only interact with its local Data Collector.

**Note**

In a network with more than one controller, it is not necessary for the data collector to be running on the same controller as the Analysis Engine.

**Note**

After an upgrade from a prior release to V8.21, the Analysis Engine will continue to interact with the Data Collectors it interacted with prior to the upgrade. Once the first In-Service scan profile is defined, the Analysis Engine will only work with data collectors (and therefore the APs) of itself and its availability partner.

Radar Functionality on the Wireless AP

A 37xx, 38xx, series 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.

When countermeasures are enabled on any of the 37xx, 38xx, series APs, they can apply them to threats discovered on the channels on which they forward traffic.

The AP371x, AP376x, and AP38xx also support Guardian mode profile. In Guardian mode, the APs rapidly sweep across multiple channels. This allows it to detect threats on channels that aren't being used by the authorized APs 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 the Analysis Engine on the controller is able to distribute responsibility for dealing with multiple concurrently active threats among multiple APs.

**Note**

If an AP is part of a WDS/Mesh link, you cannot configure it to act as a scanner 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 52). Radar capacity licenses are only required for In-Service and Guardian scan profiles. Any AP assigned to an In-Service scan profile counts as 1 against the licensed Radar capacity. The base capacity for all

controllers running V9.01 is 2 and any capacity increment can be installed on any controller running V8.21 or later.

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. A single AP can belong to at most one scan profile. Scan profiles are saved and organized based on the type of AP.

Radar provides three types of scan profiles: Legacy, In-Service, and Guardian. You can configure both In-Service and Legacy scan profiles on a single controller, but as soon as the first In-Service scan profile is created, only the host's own APs and those of its availability partner (if it has one) participate in the scans.

- AP26xx and AP36xx APs use the Legacy scan profile (for more information see [Configuring a Legacy Scan Profile](#) on page 464).
- AP37xx, AP38xx APs use the In-Service scan profile (for more information, see [Configuring an In-Service Scan Profile](#) on page 467).
- AP371X, AP3825, and AP3865 APs use the Guardian scan profile (for more information, see [Configuring a Guardian Scan Profile](#) on page 472).

Legacy Scan Profiles

Scan profiles created using the old Mitigator engine from previous releases are automatically included in Radar as Legacy scan profiles with the following differences:

- Only AP26xx and AP36xxseries APs can be assigned to a Legacy scan profile.

In-Service Scan Profiles

In-Service scan profiles work with APs based on the 37xx, 38xx architecture and includes 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 468).

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 498). If automatic blacklisting is enabled, then the administrator can:

- configure the duration that an automatically blacklisted station will remain on the blacklist
- set the maximum amount of time a device can be blacklisted.

As soon as the first In-Service scan profile is configured on a controller, the Analysis Engine will only interact with data collectors on at most 2 controllers, its host controller and its host's availability partner.

Defined and enabled Legacy scan profiles will be retained. However, the Legacy scan profile will only be applied to the APs in the profile that are active on the Analysis Engine's host or on its host's availability partner.

Guardian Scan Profiles

Guardian scan profiles work with the AP3710, AP3715, AP3825, AP376x, and AP3865 exclusively and includes the following:

An AP371x, AP376x, AP3825, AP3801, or AP3865 operating in Guardian mode does not bridge traffic and instead devotes all of the AP's resources to threat detection and countermeasures.

An AP371x, AP376x, AP3825, AP3801, or AP3865 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 AP371x, AP376x, AP3825, AP3801, or AP3865 assigned to a Guardian scan profile stops providing any services (WLAN service, load groups, site) immediately.

A list of all possible channels that the AP371x, AP3825, AP3801, AP376x, or AP3865 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 468).

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 498). 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.

As soon as the first Guardian scan profile is configured on a controller, the Analysis Engine will only interact with data collectors on at most 2 controllers, its host controller and its host's availability partner. Defined and enabled Legacy scan profiles will be retained. However, the Legacy scan profile will only be applied to the APs in the profile that are active on the Analysis Engine's host or on its host's availability partner.

Viewing Existing Scan Profiles

- 1 From the top menu, click Radar.

- 2 In the left pane, click **Scan Profiles**. The **Scan Profiles** screen displays.

The screenshot shows the 'Scan Profiles' configuration screen. The left navigation pane is expanded to 'Scan Profiles', showing a tree view with 'Legacy Scan' (containing 'smokeTestScanC411'), 'In-Service Scan' (containing 'md_1'), and 'Guardian Scan' (containing 'en_1'). The main content area displays a table with the following data:

Name	Profile	Type	Security Scan	Interference Scan	Status
<input type="checkbox"/> smokeTestScanC4110	Legacy	Active	×	N/A	Disabled
<input type="checkbox"/> en_1	Guardian	Passive	×	×	Disabled
<input type="checkbox"/> md_1	In-Service	Passive	×	×	Disabled

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

Table 109: Scan Profiles - Fields and Buttons





Field/Button	Description
Name	The name of the scan profile.
Profile	Legacy, In-Service, or Guardian.
Type	Active - Legacy scan profiles can be active, in which case the assigned APs send probe requests to speed up the discovery process Passive - Scan profiles in which the APs just listen for beacons and probe requests. In-Service scans are always passive. N/A - Only applies to In-Service and Guardian scan profiles, which always are passive.
Security Scan	Indicates whether the profile enables security scanning on APs assigned to the profile.  Indicates that the scan profile enables security scanning.  Indicates that the scan profile does not enable security scanning.

Table 109: Scan Profiles - Fields and Buttons (continued)

Field/Button	Description
Interference Scan	<p>Interference classification compares patterns in RF interference to known interference patterns to help identify the source of the interference. All APs based on the 37xx, 38xx architecture are capable of performing interference classification.</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. N/A - No interference scan classification has been applied</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> <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 463).
Delete Selected	Click to delete the selected scan profile.

Enabling the Analysis and Data Collector Engines

Before using Radar, you must enable and define the Analysis and Data Collector Engines.

If using Legacy scan profiles, up to 12 controllers can be configured (depending on the model of controller hosting the Analysis Engine) to report to the Analysis Engine. For more information, see [Configuring a Legacy Scan Profile](#) on page 464.

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 467.

To Enable the Analysis Engine:

- 1 From the top menu, click **Radar**. The **Configuration > Engine Settings** screen displays.

Controller IP	Poll Interval	Poll Retry
<input type="checkbox"/> 127.0.0.1	5	3
<input type="checkbox"/> 10.10.10.1	5	3

- 2 Enable the Analysis Engine, by selecting the **Security Analysis Engine** checkbox.

Adding a New Scan Profile

- 1 From the **Scan Profiles Summary** screen, click **New**.
- 2 In the **Add Scan Profile** dialog, select one of the following profile types from the drop-down menu:
 - Guardian
 - In-Service
 - Legacy

- 3 Configure the new scan profile as follows:
 - For a Guardian scan profile, see [Configuring a Guardian Scan Profile](#) on page 472.
 - For an In-Service scan profile, see [Configuring an In-Service Scan Profile](#) on page 467.
 - For a Legacy scan profile, see [Configuring a Legacy Scan Profile](#) on page 464.

Configuring a Legacy Scan Profile

Once a new Legacy scan profile is created, the General Tab displays.

The screenshot shows the configuration interface for a Legacy Scan Profile. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar shows the Configuration menu with Scan Profiles expanded, listing Legacy Scan (smokeTestScanC4110), In-Service Scan (md_1), and Guardian Scan (en_1). The main content area is titled 'Scan Profile: smokeTestScanC4110' and has two tabs: 'General' (selected) and 'Assigned APs'. The General tab contains the following fields and controls:

- Name:** smokeTestScanC4110
- Radio:** Both (dropdown)
- Channel List:** All (dropdown)
- Scan Type:** Active (dropdown)
- Channel Dwell Time:** 250 ms
- Scan Time Interval:** 15 min
- Security Scan:**
- Scan Activity:** Disabled

At the bottom of the General tab are three buttons: 'Start Scan', 'Stop Scan', and 'Run Now'. A red warning message states: '* Enabling scanning may disrupt client services'. At the bottom of the configuration area are 'New', 'Delete', and 'Save' buttons.

Table 110: General Tab - Fields and Buttons

Field/Button	Description
Name	Type a unique name for this scan profile.
Radio	From the drop-down list, click one of the following: <ul style="list-style-type: none"> Both - Radio 1 and Radio 2 both perform the scan function. radio 1 - Only Radio 1 performs the scan function. radio 2 - Only Radio 2 performs the scan function.
Channel List	From the drop-down list, click one of the following: <ul style="list-style-type: none"> All - Scanning is performed on all channels. Current - Scanning is performed on only the current channel.
Scan Type	From the drop-down list, click one of the following: <ul style="list-style-type: none"> Active - The AP sends out Probe Requests and waits for Probe Response messages from any access points. Passive - The AP listens for 802.11 beacons.
Channel Dwell Time	Type the time (in milliseconds) that an AP spends on a channel during one pass of a Legacy scan. The Legacy AP makes one pass through its list of channels, spending the channel dwell time on each of them.

Table 110: General Tab - Fields and Buttons (continued)

Field/Button	Description
Scan Time Interval	Type the time (in minutes) to define the frequency at which an AP within the Scan Group will initiate a scan of the RF space. The range is between 10 minutes and 120 minutes.
Security Scan	Click to enable scanning for the assigned APs.
Scan Activity	Displays the current state of the security scan.
Start Scan	Click to start the security scan which runs the scan according to the schedule in the Analysis Engine database at the time the scan is initiated (for more information, see Running/Saving a Legacy Scan on page 466).
Stop Scan	Click to stop the security scan.
Run Now	Click to run 1 pass of the security scan.

Viewing the List of Assigned APs

The list of Assigned APs is a complete list of APs local to the controller and automatically appear once a scan profile is created. To view a list of APs assigned to this Legacy scan profile, click the **Assigned APs** tab.



Note

If an AP is part of a WDS/Mesh you cannot configure it to act as a scanner in Radar.

The screenshot shows the 'Radar' tab in the Identifi management console. The main content area displays the configuration for a scan profile named 'smokeTestScanC4110'. The 'Assigned APs' tab is active, showing a table with the following data:

Wireless APs		Controller	R1	R2
<input type="checkbox"/>	C4110 - ap1 - AP4102 *	Local Controller	a	b/g
<input type="checkbox"/>	C4110 - ap2 - AP3620 *	Local Controller	a/n	b/g

At the bottom of the table, there is a legend: † Inactive APs * Scanning not allowed. Below the table are buttons for 'New', 'Delete', and 'Save'.

Table 111: Assigned APs Tab - Fields and Buttons

Field/Button	Description
Wireless APs	Identifies the wireless APs assigned to this Legacy scan profile. May include the AP name or serial number.
Controller	Identifies the controller associated with the wireless AP. An IP address indicates a controller outside the network; "Local Controller" indicates that the AP is active on the controller hosting the Analysis Engine.
R1	Status of Radio 1.
R2	Status of Radio 2.
New	Click to create a new Legacy scan profile. For more information, click Adding a New Scan Profile on page 463.
Delete	Click to delete the selected Legacy scan profile.
Save	Click to save changes.

To assign an AP to a Legacy scan profile

The Assigned APs tab is used to manage which APs are assigned to the profile. The list contains all the APs that are eligible to be assigned to the profile.

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Scan Profiles**. The **Scan Profiles** screen displays.
- 3 Select a Legacy scan profile, and click the **Assigned APs** tab.
- 4 Select an AP from the list of Assigned APs.

**Note**

Only AP26xx and AP36xx series APs can be assigned to a Legacy scan profile.

- 5 Click **Save**.

**Note**

Saving a scan profile does not start Legacy scanning.

Running/Saving a Legacy Scan

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Scan Profiles**. The **Scan Profiles** screen displays.
- 3 Select a Legacy scan profile. The General tab is displayed.
- 4 Click **Security Scan**.

- To run a Legacy scan, click one of the following:
Run Now, which runs 1 pass of the scan, or

Start Scan which runs the scan according to the schedule in the Analysis Engine database at the time the scan is initiated.



Note

You must click **Save** to save configuration changes even if you have also pressed Start Scan or Run Now.

- To save the Legacy scan, click **Save**.
- To stop the scan, click **Stop**.

Configuring an In-Service Scan Profile

Once a new In-Service Scan Profile is created, the **Detection** tab displays.

In-Service Scan Profile Detection Settings

The screenshot shows the Identifi Radar web interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar shows the Configuration menu with Scan Profiles expanded, listing Legacy Scan (smokeTestScanC411), In-Service Scan (md_1), and Guardian Scan (en_1). The main content area is titled 'Scan Profile: md_1' and has three tabs: Detection, Prevention, and Assigned APs. The Detection tab is active, showing a 'Name' field with 'md_1' and three checkboxes: 'Scan for security threats', 'Rogue AP detection' (with a 'Listener port' field set to '348 (1-32768)'), and 'Classify sources of interference'. At the bottom of the main area are 'New', 'Delete', and 'Save' buttons.

- 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 494).
- 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.



Note

This feature is not supported on the 36xx or 26xx series APs.

- 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, and AP38xx architecture are capable of performing interference classification.

2 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 459.

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 493.

Selecting Countermeasures

Countermeasures mitigate the impact of a security threat. Three main countermeasures are used by the 37xx, 38xx series 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.

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**. The **Scan Profiles** screen displays.

3 Select an In-Service scan profile and click the **Prevention** tab.

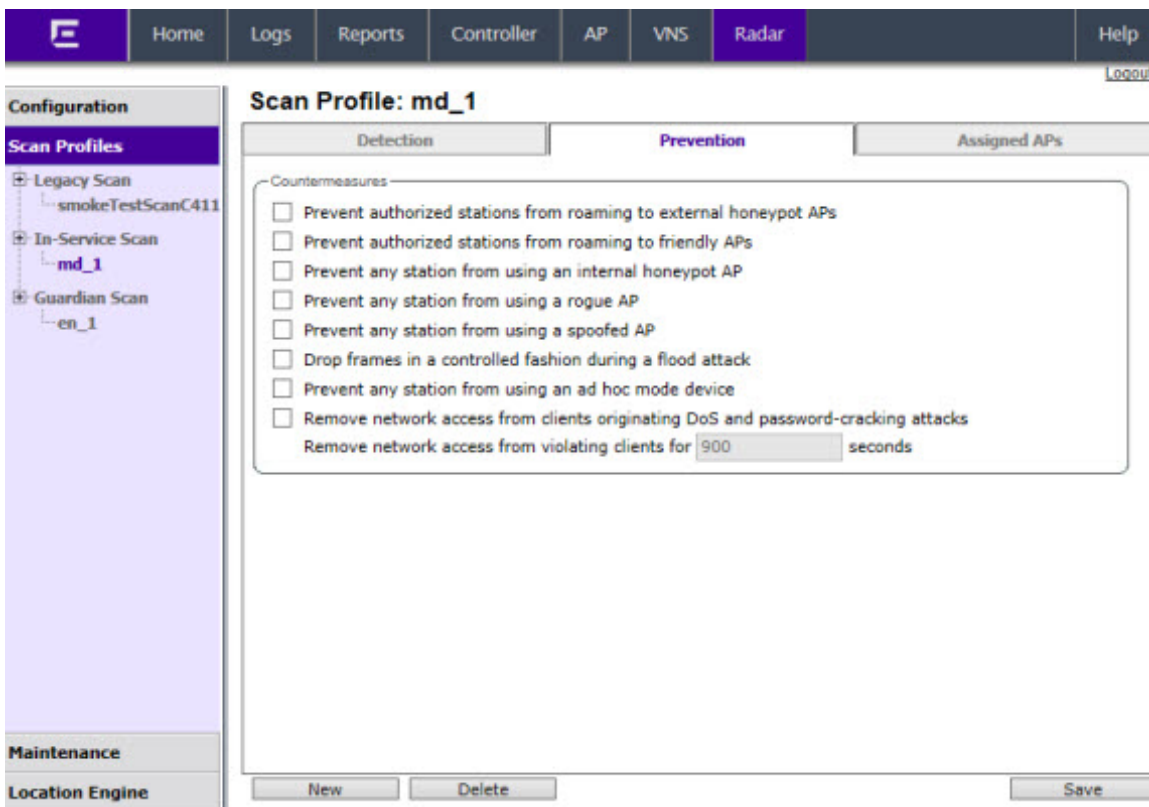


Table 112: Prevention Tab - Fields and Buttons

Field/Button	Description
Countermeasures	
Prevent authorized devices 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 devices 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.
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.

Table 112: Prevention Tab - Fields and Buttons (continued)

Field/Button	Description
Drop frames in a controlled fashion during ad hoc mode	Drop frames are not dropped from ad hoc mode clients directly. Deauthentication messages are used to prevent devices from using an ad hoc mode device.
Remove network access from clients originating DoS 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.
Remove network access from violating clients for a period of time	Prevents clients from successfully associating to any authorized APs. This is particularly useful for preventing devices performing active password cracking attacks from successfully brute forcing a password.
New	Click to create a new scan profile. For more information, click Adding a New Scan Profile on page 463.
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 a complete list of APs local to the controller and 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.

Table 113: 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 controller outside the network, Local Controller indicates a controller local to the AP.
New	Click to create a new In-Service scan profile. For more information, click Adding a New Scan Profile on page 463.
Delete	Click to delete the selected In-Service scan profile.
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.

To assign an AP to an In-Service scan profile:

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Scan Profiles**. The **Scan Profiles** screen displays.
- 3 Select an In-Service scan profile, and click the **Assigned APs** tab.
- 4 Select an AP from the list of Assigned APs.

- Click **Save**.



Note

Only AP37xx, and AP38xx series APs use the In-Service scan profile.

Configuring a Guardian Scan Profile

Once a new Guardian Scan Profile is created, the Detection tab displays.

Guardian Scan Profile Detection Settings

- 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 494).
- 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 architecture are capable of performing interference classification.

- 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 459.

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 493.

Selecting Countermeasures

Countermeasures mitigate the impact of a security threat. Three main countermeasures are used by the 371x series APs by Guardians:

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

- 3 Select a Guardian scan profile and click the **Prevention** tab.

- 4 Select desired Prevention method .
- 5 Select number of Channels per radio to defend concurrently. Number of defended channels can be between 1 and 4.

Table 114: Prevention Tab - Fields and Buttons

Field/Button	Description
Countermeasures	
Prevent authorized devices 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 devices 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 s 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 114: 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.
Drop frames in a controlled fashion during ad hoc mode	Drop frames are not dropped from ad hoc mode clients directly. Deauthentication messages are used to prevent devices from using an ad hoc mode device.
Remove network access from clients originating DoS 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.
Remove network access from violating clients for a period of time	Prevents clients from successfully associating to any authorized APs. This is particularly useful for preventing devices performing active password cracking attacks from successfully brute forcing a password.
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 463.
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 complete list of APs local to the controller and APs from the availability partner. 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.

Table 115: Assigned APs Tab - Fields and Buttons

Field/Button	Description
Wireless APs	Identifies the wireless APs assigned to this Guardian scan profile. May include the AP name or serial number.
Controller	Identifies the controller associated with the wireless AP. An IP address indicates a controller outside the network, 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.
New	Click to create a new Guardian scan profile. For more information, click Adding a New Scan Profile on page 463.
Delete	Click to delete the selected Guardian scan profile.
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.

To assign an AP to a Guardian scan profile:

- 1 From the top menu, click **Radar**.
- 2 In the left pane, click **Scan Profiles**. The **Scan Profiles** screen displays.
- 3 Select a Guardian scan profile, and click the **Assigned APs** tab.
- 4 Select an AP from the list of Assigned APs.

- 5 Click **Save**.

**Note**

Only AP371x APs use the Guardian scan profile.

Maintaining the Radar Lists of APs

Radar provides a list of APs organized by 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 almost any other using Radar (for more information, see [Reclassifying APs](#) on page 485).

AP Categories

APs are labeled as belonging 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 based on the AP37xx, and AP38xx architecture can prevent authorized devices from using friendly APs.
- **Uncategorized APs** - APs discovered by scanning APs and which do not fall into any other category.
- **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 In the left pane, click **Maintenance**. The **Scanning APs** screen displays.

The screenshot shows the IdentifiFi Radar interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, Radar, and Help. The left sidebar has Configuration, Scan Profiles, Maintenance (selected), Scanning APs, Friendly APs, Uncategorized APs, Authorized APs, Prohibited APs, and Location Engine. The main content area is titled 'Scanning APs' and contains a table with the following structure:

Wireless Controllers	Wireless APs		
Name	Serial	Profile Name	Licensed
> In-service Scan Profile Guardian Scan Profile			

Table 116: Scanning APs - Fields and Buttons

Field/Button	Description
Wireless Controllers	Name - 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	Profile Name - Description of the Access Point
	Serial - Serial number of the Access Point

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 In the left pane, under Maintenance, click **Friendly APs**. The **Friendly APs** screen displays.

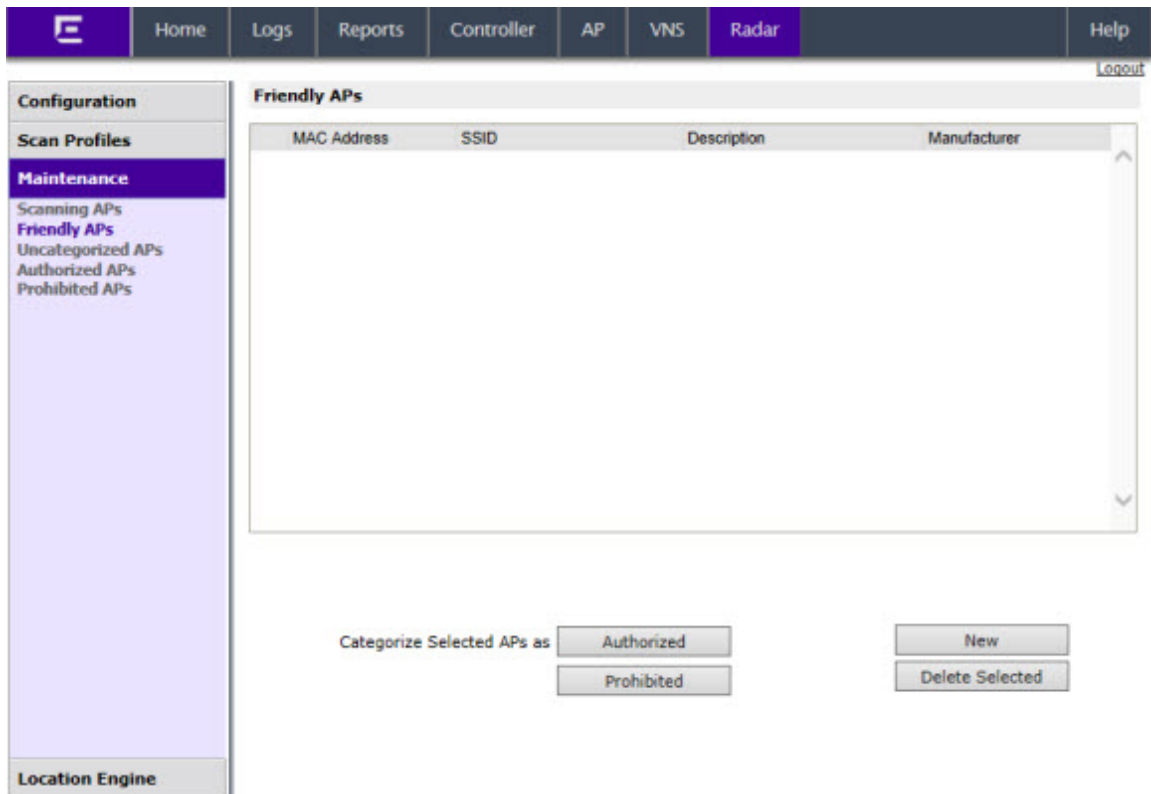


Table 117: Friendly APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address for the friendly AP
SSID	Specifies the SSID for 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 485.
New	Click to create a new Friendly AP. For more information, see Adding Friendly APs on page 479.
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 To add friendly access points manually to the **Friendly APs** list, click **New**. The **Edit Threat AP** dialog displays.

Edit threat AP ? X

MAC Address:

SSID:

Description:

Save **Cancel**

- 2 In the Edit Threat AP dialog, type the following:
 - **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
- 3 Click **Save**. The new access point is displayed in the Friendly APs list.

Modifying Friendly APs

To Modify a Friendly AP:

- 1 From the top menu, click **Radar**. The **Radar** screen displays.
- 2 In the left pane, under Maintenance, click **Friendly APs**. The **Friendly APs** screen displays.
- 3 In the **Friendly APs** list, double-click the access point you want to modify.
- 4 In the **Edit threat AP** dialog, modify the access point as required.

Edit threat AP ? X

MAC Address:

SSID:

Description:

Save **Cancel**



Note

The MAC Address field cannot be modified

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

Viewing the List of Uncategorized APs

The list of 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**.

- In the left pane, under Maintenance, click **Uncategorized APs**. The **Uncategorized APs** screen displays.

MAC Address	SSID	Manufacturer
<input type="checkbox"/> 00:0F:CB:00:A1:E1	suwlan	Chantry Networks
<input type="checkbox"/> 00:0F:CB:00:CB:DE	home	Chantry Networks
<input type="checkbox"/> 00:1A:EB:35:AC:B1	11d11h	Siemens Enterprise Communications GmbH & Co. KG
<input type="checkbox"/> 00:0E:8C:9B:FB:3A	cnf107b-bap	Siemens AG ASD ET
<input type="checkbox"/> 00:00:00:1E:A0:09	11d11h	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:CB:00:AA:29	suwlan	Chantry Networks

Categorize Selected APs as

Authorized

Friendly

Prohibited

Table 118: Uncategorized APs Screen - Fields and Buttons

Field/Button	Description
MAC Address	Specifies the MAC address of the uncategorized AP
SSID	Specifies the current operating channel of 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 485.

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:

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

- 2 In the left pane, under Maintenance, click **Authorized APs**. The **Authorized APs** screen displays.

The screenshot shows the 'Authorized APs' screen. The left navigation pane is under 'Maintenance' and includes 'Authorized APs'. The main content area displays a table with the following data:

MAC Address	Description	Manufacturer
<input type="checkbox"/> 20:B3:99:43:29:18	dwwdwd	Enterasys
<input type="checkbox"/> 00:1F:45:95:42:D9	dtesedwd12	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

Below the table, there are three buttons: 'Categorize Selected APs as Friendly', 'New', and 'Delete Selected'.

Table 119: 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 485.
New	Click to create a new authorized AP. For more information, see Adding Authorized APs on page 482.
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 since the controllers will do it automatically. However, there may be times when you 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 standalone AP or 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 Edit Authorized AP dialog displays.



The screenshot 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 text input fields. The first is labeled "MAC Address:" and the second is labeled "Description:". 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 In the left pane, under Maintenance, click **Prohibited APs**. The **Prohibited APs** screen displays.

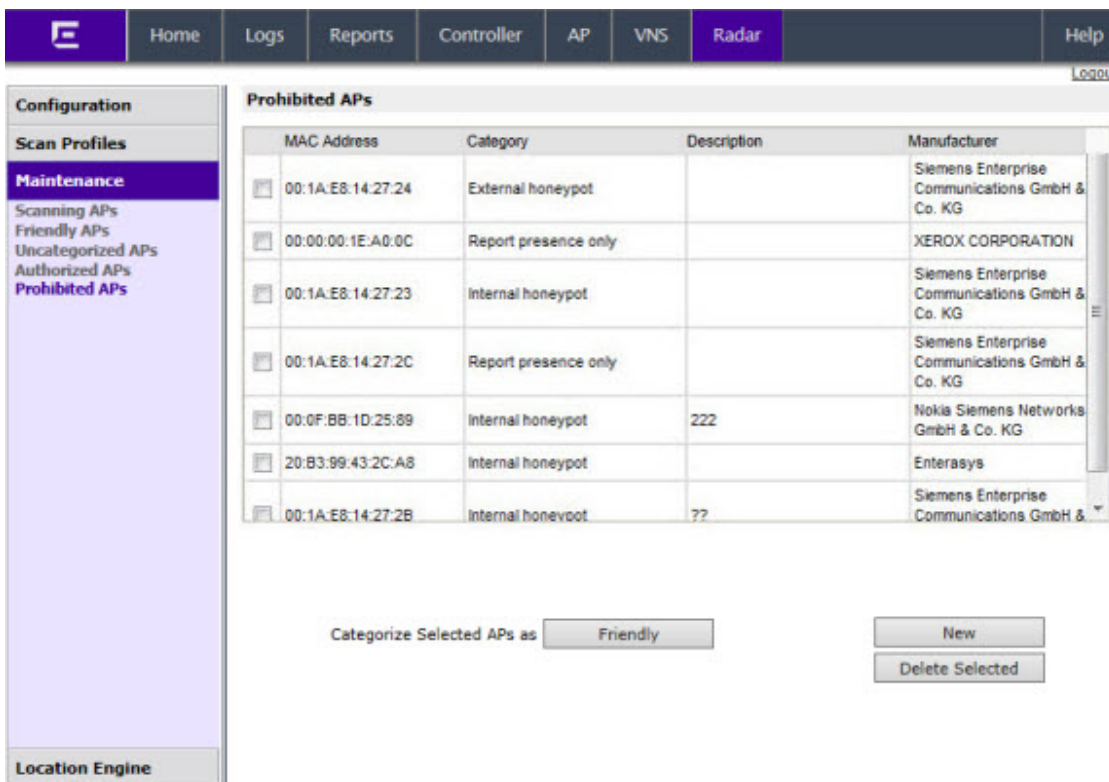


Table 120: Prohibited APs Screen - Fields and Buttons

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 485.
New	Click to create a new prohibited AP. For more information, see Adding Prohibited APs on page 484.
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 friendly access points manually to the **Prohibited APs** list, from the Prohibited APs screen, click **New**. The Prohibited APs dialog displays.

Prohibited APs [?] [X]

MAC Address:

Description:

Action:

- Report presence only
- Treat like an internal honeypot AP
- Treat like an external honeypot AP

- 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.

Reclassifying APs

APs listed as friendly or uncategorized, can be reclassified as authorized.

To Reclassify APs as Authorized:

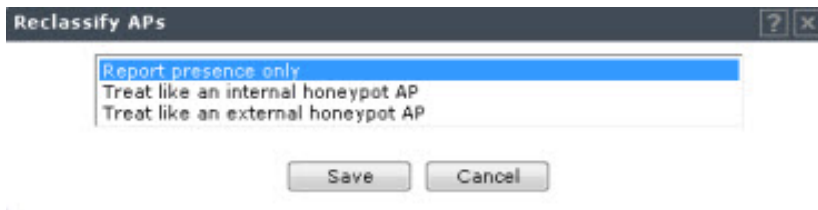
- 1 From the top menu, click **Radar**. The Radar screen displays.
- 2 In the left pane, under Maintenance, click **Friendly APs** or **Uncategorized APs**. The selected list of APs is displayed.
- 3 Select the desired APs from the list of APs.
- 4 Click **Authorized**.
- 5 Click **OK** to reclassify the selected AP.

To Reclassify APs as Threats

APs listed as friendly or uncategorized, can be reclassified as threats.

- 6 From the top menu, click **Radar**. The Radar screen displays.
- 7 In the left pane, under Maintenance, click **Friendly APs** or **Uncategorized APs**. The selected list of APs is displayed.

- 8 To reclassify an AP as a “threat”, select the APs from the list of APs and click **Prohibited**. The **Reclassify APs** dialog displays. For more information, see [In-Service Scan Profile Prevention Settings](#) on page 468.



- 9 Select a threat classification from the list displayed.
- 10 Click **Save**.

To Reclassify as Friendly APs:

APs listed as uncategorized, authorized, or prohibited, can be reclassified as friendly.

- 11 From the top menu, click **Radar**. The Radar screen displays.
- 12 In the left pane, under Maintenance, click **Uncategorized APs, Authorized APs, or Prohibited APs**. The selected list of APs is displayed.
- 13 To reclassify an AP as “friendly”, select the APs from the list of APs and click **Friendly**.
- 14 Click **OK** to reclassify the selected AP.

Configuring the Location Engine

The Radar Location Engine provides suggested AP locations on a floor plan based on signals received from sets of distances (Received Signal Strength (RSS)). A library provides mapping of APs on a given floor to fingerprint (heat map) for locating various stations based on RSS. Access points scattered on a given floor scan the air in various channels and report the received RSS from various stations to the controller.



Note

The Location Engine is not the preferred method for managing floor plan files. Therefore, it is recommended that you use NetSight OneView Maps for complete management of floor plan files for the controller. For more information, see the NetSight OneView User documentation.

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, click **Location Engine**.

Table 121: 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)
Location Targets	
Locate active sessions	Click to locate all active users located within the signal range.
Track Area Change	Click to track client locations within pre-defined areas using the Location Engine. When the clients change areas, a notification is sent.
On-demand Users	Displays a list of on-demand users.
Add	Click to create a new On-demand User. For more information, see Creating a New On-Demand User on page 489

Table 121: Location Engine Settings Dialog - Fields and Buttons (continued)

Field/Button	Description
Delete Selected	Click to delete the selected On-Demand User.
Advanced button	Click to open the Advanced dialog, see Downloading a Floor File on page 489
Save	Click to save changes.

Location Batch Reporting

- 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 Batch Reporting, click **Location Batch Reporting**.

The screenshot shows the 'Location Batch Reporting' settings dialog. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. The left sidebar shows 'Configuration', 'Scan Profiles', 'Maintenance', and 'Location Engine' (selected), with sub-items 'Location Engine Settings' and 'Location Batch Reporting'. The main content area has a checked checkbox for 'Location Batch Reporting'. Below it, there is a field 'Report all station locations every' with a dropdown set to '60' and the unit 'minute(s)'. The 'Dimension Unit' is set to 'Meter'. A section titled 'Post all location destinations to the following URLs:' contains a text area for 'Destination URL' and 'Add' and 'Delete Selected' buttons. A 'Save' button is located at the bottom right.

Table 122: Location Batch Reporting Settings Dialog - 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.
Destination URL	List of destination URLs.

Table 122: Location Batch Reporting Settings Dialog - Fields and Buttons (continued)

Field/Button	Description
Add	Click to create a new Destination URL. For more information, see Creating a New Destination URL on page 489.
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**.
- 3 Click **Location Batch Reporting**.
- 4 The **Location Batch Reporting** screen displays.
- 5 Click **Add**. The **Destination URL** dialog displays.

- 6 Enter a URL for the new Destination.
- 7 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.

- 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
? x

Show 10 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 ◀ ▶

Download...
Upload Selected...
Delete Selected...

¹To 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
? x

Protocol: FTP

Server:

User ID:

Password:

Confirm:

Directory:

Filename:

Download
Close

Table 123: 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, showing Floor ID 1, Floor Name Thornhill, Number of APs 9, Cell Size 100X100, Number of Cells 2035, Width 3700, Length 5500, and Type of Environment Model 4. Below the table are buttons for 'Download...', 'Upload Selected...', and 'Delete Selected...'. A 'Close' button is at the bottom. A search bar and 'Show 10 entries' are at the top.

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 ◀ ▶

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.

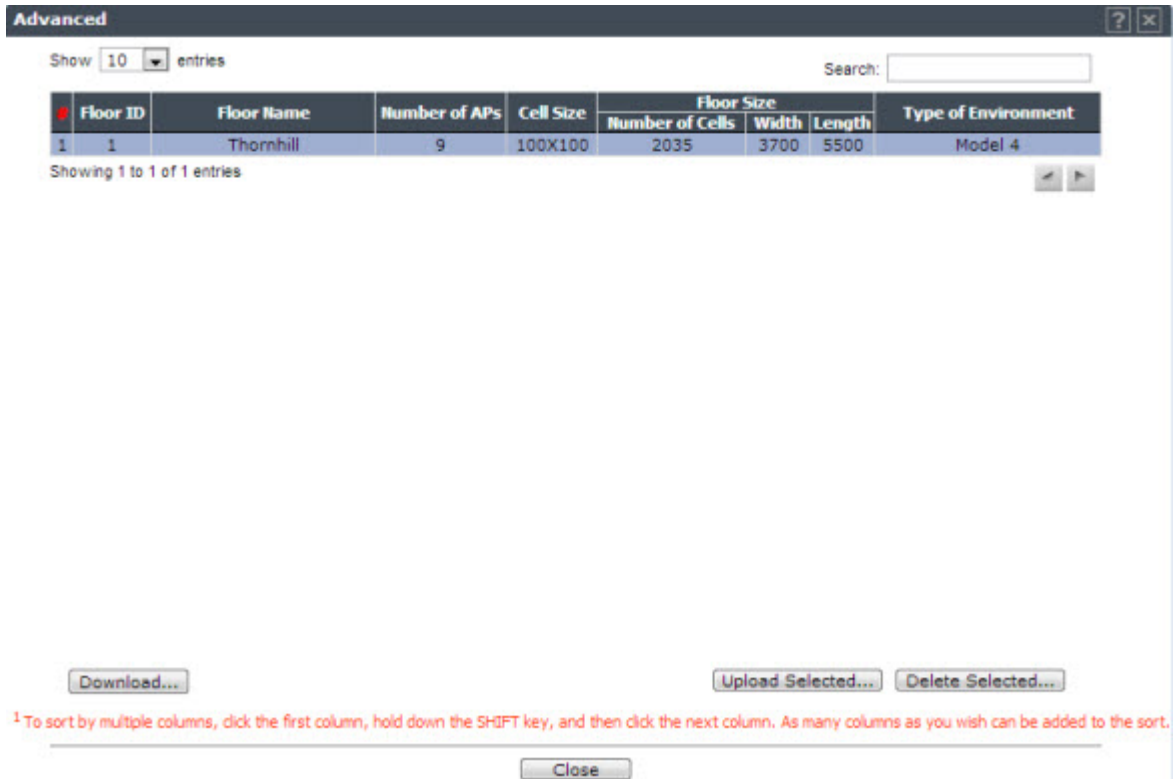
Table 124: Upload Floor Plan File Dialog - Fields and Buttons

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

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

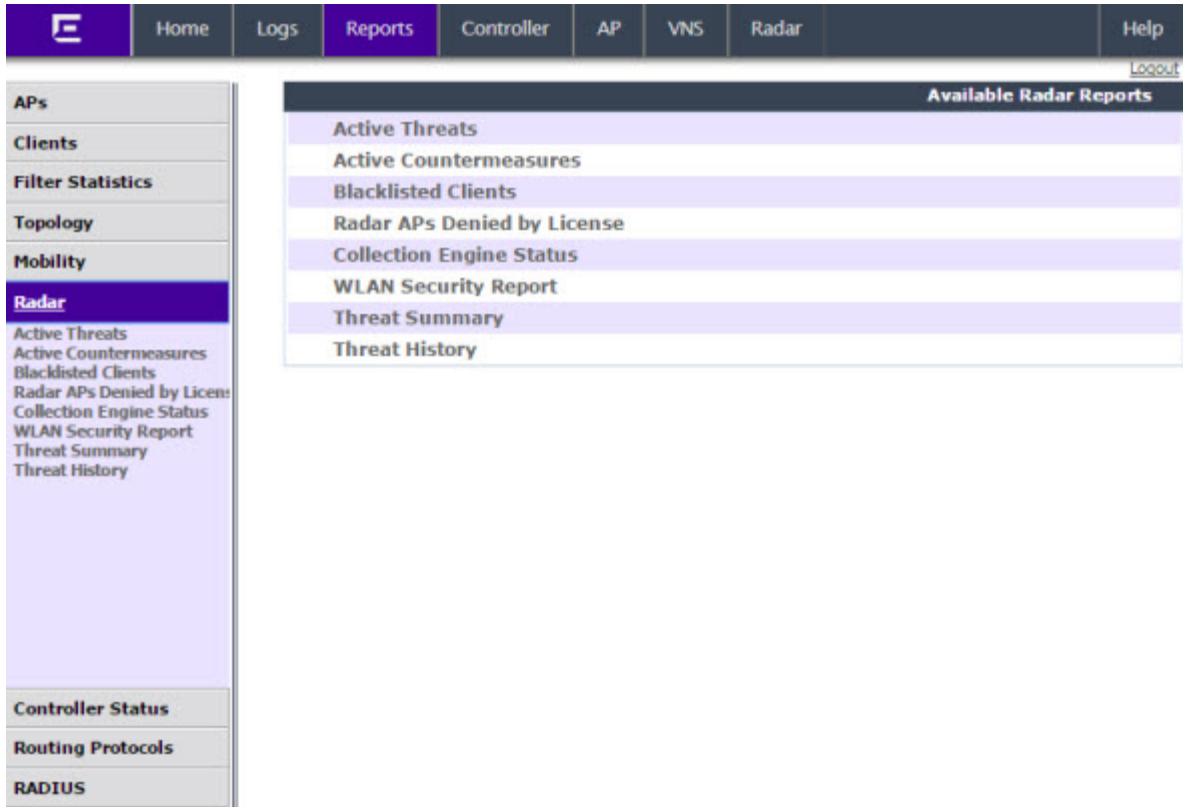
- 4 Select a floor file from the list of floor files. Only one floor file can be deleted at a time.
- 5 Click **Delete Selected** to delete the floor file from the list. Click **OK** to confirm the delete operation.
- 6 Click **Close**.

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**. The **Available Radar Reports** screen displays.



- 3 Click on the desired report:
 - [Active Threats](#) on page 495
 - [Active Countermeasures](#) on page 497
 - [Blacklisted Clients](#) on page 498
 - [Radar APs Denied by License](#) on page 499
 - [Collection Engine Status](#) on page 499
 - [WLAN Security Report](#) on page 500
 - [Threat Summary](#) on page 501
 - [Threat History](#) on page 502

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.
- **Rogue 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 502).

Viewing Active Threats Scan Results

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Reports**. The **Available Radar Reports** screen displays.
- 3 Click **Active Threats**. The **Active Threats Report** screen displays.

lab-422-g - Reports - Active threats report
 No refresh Refresh every secs

Showing 0 to 0 of 0 entries Search:

Detected Active At	Threat MAC Address	Threat	Threat Category	Countermeasures Applied	Location		Additional Details
					AP Name	RSS	
No data available in table							

Showing 0 to 0 of 0 entries ◀ ▶

Data as of Mar 03, 2014 09:37:54 am Selected Threats

Table 125: 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 494.
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. 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 (DHCP is through the Rogue AP). 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 126: 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 495.
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 127: 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**. The **Available Radar Reports** screen displays.
- 3 Click **Radar APs Denied by License**. The following screen displays.

Assigned APs	Scan profile
LAB42-AP3705i	is
LAB46-AP3825i	is

Table 128: 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.

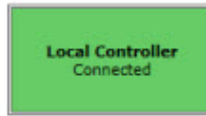
Collection Engine Status

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**. The **Collection Engine Status** screen displays.

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**. The **Available Radar Reports** screen displays.
- 3 Click **WLAN Security Report**. The **WLAN Security Report** is displayed.

identifi™ Radar

WLAN Security Report

For Controller lab-422-g (192.168.14.11)
Release 9.01
Generated on March 3, 2014

Extreme
networks

WLAN Se

Introduction

This report identifies security-related problems in the configuration of the controller EWC's WLAN provides guidance for their resolution.

Issue Summary

Table 1: Counts of WLAN Services and WLAN Services with Issues

	Enabled Services	Disabled Services
WLAN Service	19	0
WLAN Service with Issues	8	0

Distribution of Issues

Enabled WLANs

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**. The **Available Radar Reports** The screen displays.
- 3 Click **Threat Summary**. The **Threat Summary** is displayed.

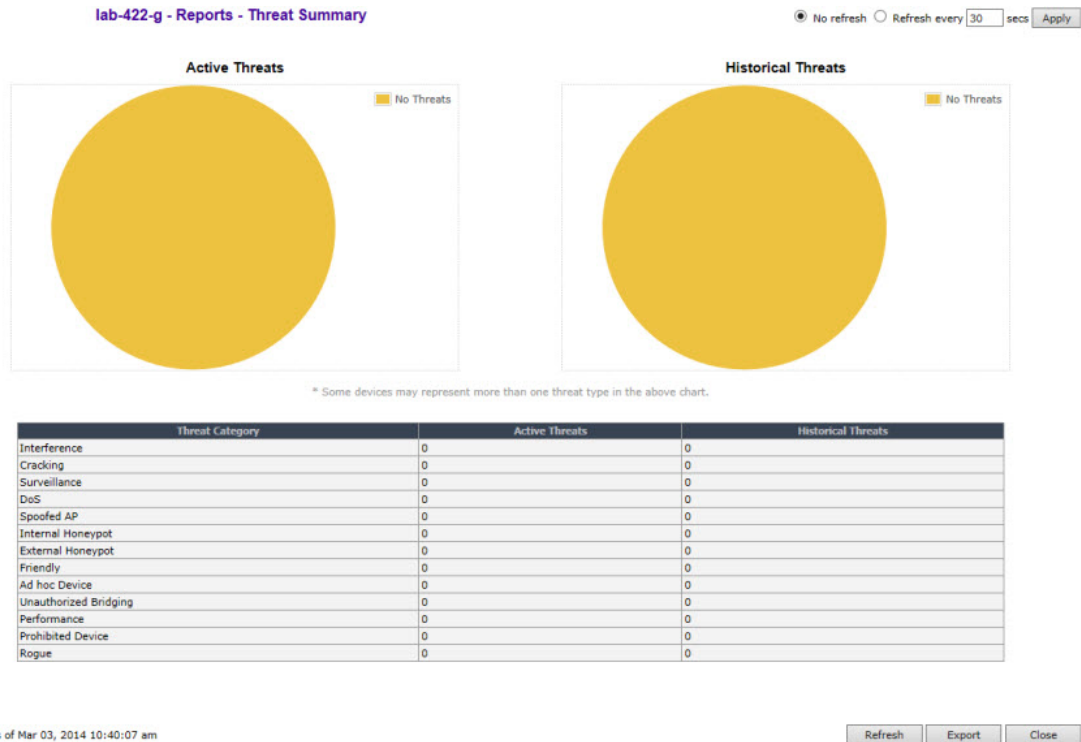


Table 129: Threat Summary Report - Fields and Buttons

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 494.
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**. 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**.

Threat History

Viewing the Threat History

- 1 From the top menu, click **Reports**.
- 2 In the left pane, click **Reports**. The **Available Radar Reports** screen displays.
- 3 Click **Threat History**. The **Threat History** screen displays.

lab-422-g - Reports - Historical threat report

Showing 0 to 0 of 0 entries

Search:

Last Reported	First Detected	Threat MAC Address	Threat	Threat Category	Currently Active	Location		Additional Details
						AP Name	RSS	
No data available in table								

Showing 0 to 0 of 0 entries

Data as of Mar 03, 2014 10:42:10 am

Table 130: 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 495.
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 Reports and Statistics

Available Reports and Statistics
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
Viewing RADIUS Reports
Call Detail Records (CDRs)

Available Reports and Statistics

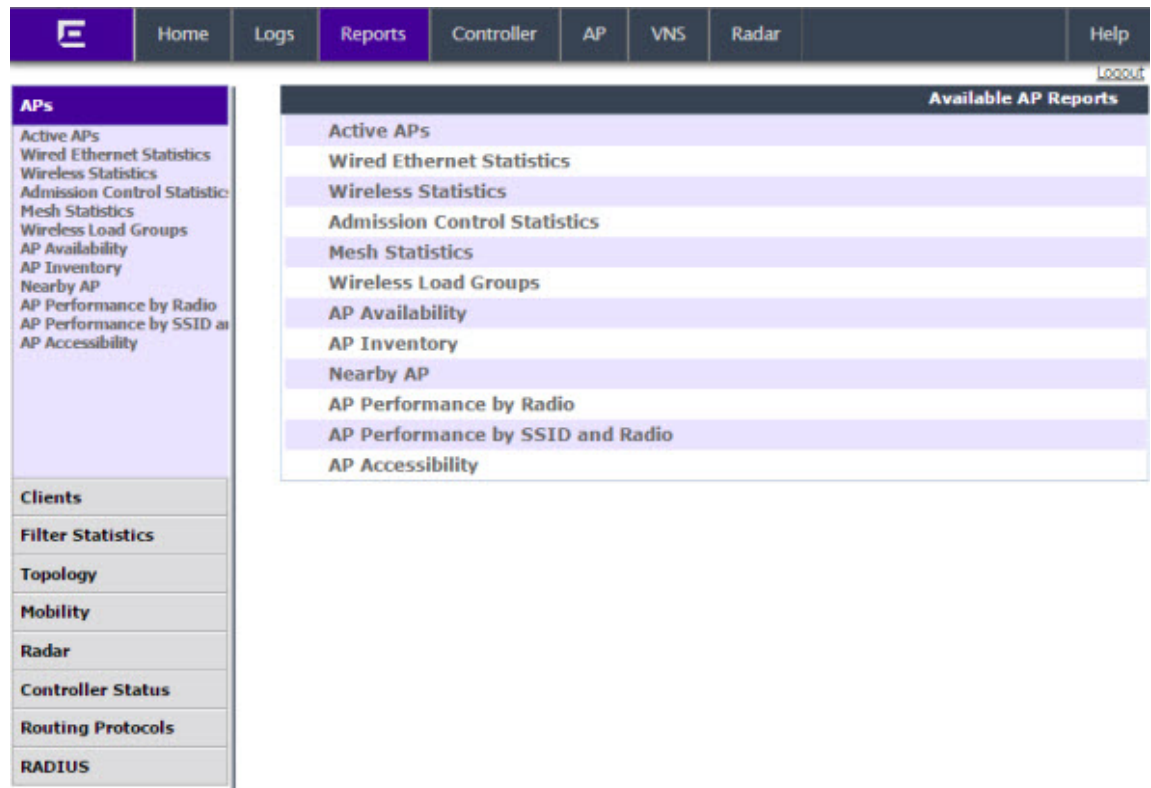
The following reports and statistics are available:

- AP Reports
- Active Clients Reports
- Filter Statistics Reports
- Topology Reports
- Mobility Reports
- Controller Status Reports
- Routing Protocols Reports
- RADIUS Reports

Viewing AP Reports and Statistics

To View AP Reports and Statistics:

From the top menu, click **Reports**. The **Available AP Reports** screen displays.



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
- Nearby AP
- AP Performance by Radio
- AP Performance by SSID and Radio
- AP Accessibility

The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

The following Available Active Clients Reports allow you to search for clients, either by user name, MAC address, or IP address that are associated to the APs.

- Active Clients by AP

- Active Clients by VNS
- All Active Clients

You can also use the **Select All** and **Deselect All** buttons for selecting the active Wireless APs on those displays.

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**. The **Available AP Reports** screen displays.
- 2 Click the **Active APs** display option. The **Active Wireless APs** display opens in a new browser window.

lab-422-g - Reports - Active Wireless APs No refresh Refresh every secs

Wireless AP	Serial	AP IP	Clients	Home	Role	Mesh/WDS Children ¹	Sec. Tunnel ²	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	Capture Timeout	Invalid Role
C4110 - ap1 - AP4102	0002000609223321	10.219.40.10	0	Local	Traffic forwarder (AP)	1	N/A	4:40:35	796565	1486494	95324206	2066244813	6:20:06	N/A	0
C4110 - ap2 - AP3620	0500008043050317	10.219.40.13	1	Local	Traffic forwarder (AP)	0	SCD	4:39:51	222789	393150	-	-	5:51:54	off	0
Summary	2 active APs		1												

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 Mar 03, 2014 10:49:29 am

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.

lab-422-g - Reports - Active Clients by Wireless AP No refresh Refresh every secs

Users	AP	Client IP	Client MAC	ESS MAC	SSID	Auth. Prio.	Radio	Protocol	RSS (dBm)	User	Time Conn.	Roaming	Role	Default Action	Phys	Avg. Rate (Mbps)	Packets Sent/Rec'd	Bytes Sent/Rec'd	DL Emitted Over Tx Rate	DL Dropped Over Tx Rate	Packets/Bytes
C4110 - ap1 - AP4102	0	No Client is connected to this Wireless AP																			
C4110 - ap2 - AP3620	1	No Client is connected to this Wireless AP																			

¹ L1DPG, S1STRG, T1VMP

Active Users: 0
 Auth Users: 0
 Non-Auth Users: 0

Search Client by:

Data as of Mar 03, 2014 11:12:34 am Selected clients:

- 3 In the **Wired Ethernet Statistics by Wireless AP** display, click a registered AP to display its information.
- 4 Click LAG Detail. The LAG Details dialog opens and the following Ethernet LAG information is displayed:
 - Actor System ID
 - Actor Admin key
 - Actor Oper key
 - Actor System Priority
 - Partner System ID
 - Partner Oper key
 - Partner System Priority

Viewing Wireless Statistics:

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.
- 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 **AP Status:** Approved **AP IP Address:** 10.219.40.10

C4110 - ap2 - AP3620

		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**. The **Available AP Reports** screen displays.

- 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 002000609223321

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**. The **Available AP Reports** screen displays.

- 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**. The **Available AP Reports** screen displays.
- 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.

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			

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

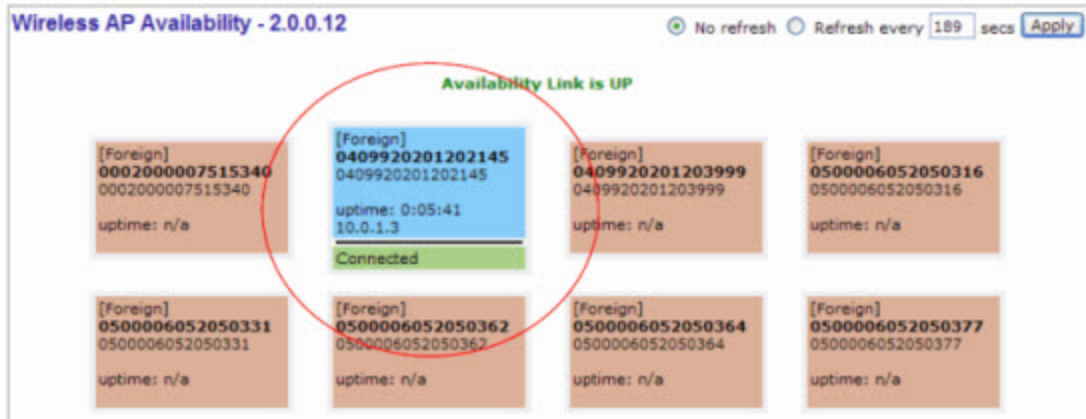
The current controller is the one on which the AP Availability report is viewed.

- 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**. The **Available AP Reports** screen displays.
- 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:

lab-422-g - Reports - Wireless AP Inventory

Data as of Mar 03, 2014 11:02:28 am

Wireless AP (Serial)	Topology			HW				SW		Country	Antennas			Sec. Tunnel	Cert.	Telnet/SSH	LBS	Mcast Assembly	BD	Persistence		
	Rdo	Ra	Rb	Rg	Rn	DP	BP	RT	FT	Req Ch	Ch / Tx	Aj	TxMn	TxMx	ATT	Dom	MnBR	MxBR	MxOR	RxDV	TxDV	
	11n Channel Width				11n Guard Interval				11n Protection Mode				Failure Maintn.		Assn	IP Address	Netmask		Gateway		MTU Interface	MTU Tunnel
C4110 - ap1 - AP4102 (0002000609223321) Role: Traffic forwarder(AP)	Port1			Wireless AP4102				09.01.01.0207T		United States	left-1: Integrated antenna middle-1: N/A right-1: Integrated antenna left-2: N/A middle-2: N/A right-2: N/A			-	-	disabled	enabled	disabled	disabled	disabled	disabled	
	1	on	-	-	off	5	100	2346	2346	157	157/10 dBm	-	3 dB	10 dB	-	MyDomain	6 Mbps	24 Mbps	54 Mbps	Best	Alternate	
	-				-				-				-		-		-		-		-	
2	-	on	on	off	5	100	2346	2346	3	3/10 dBm	-	8 dB	10 dB	-	MyDomain	1 Mbps	11 Mbps	54 Mbps	Best	Alternate		

Table 131: AP Inventory Report Columns on page 513 lists the column names and abbreviations found in the AP Inventory report:

Table 131: 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
Sec. Tunnel	Secure tunnel mode
Cert.	AP certification (enabled or disabled)
Telnet/SSH	Telnet or 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.
Wired MAC	The physical address of the AP's wired Ethernet interface.
Description	As defined on the AP Properties screen.

Table 131: AP Inventory Report Columns (continued)

Column Name	Description
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
Dom	RF domain
MnBR	Minimum Basic Rate (For more information, see the Wireless AP radio configuration tabs.)
MxBR	Maximum Basic Rate
MxOR	Maximum Operational Rate
RxDV	Receive Diversity
TxDV	Tx Diversity
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 131: 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.

Nearby AP Report

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.
- 2 Click the **Nearby AP** display option. The **Nearby APs** display opens in a new browser window.

EWC - Reports - Nearby AP Report No refresh Refresh every 30 secs

AZ3705i-AZ
AZ3825i-AZ
AZ3865e-AZ

Channel: 11: (2462)
Last Scan: 2/20/2015 11:21:16

Nearby AP	BSSID	Channel	RSS
Unknown	00:01:02:03:04:08	11: (2462)	-85
Unknown	00:1A:E8:14:24:78	11: (2462)	-69
Unknown	00:1A:E8:14:24:79	11: (2462)	-69
Unknown	00:1F:45:80:D5:D8	11: (2462)	-32
Unknown	00:1F:45:80:D5:D9	11: (2462)	-32
Unknown	00:1F:45:80:D5:DA	11: (2462)	-31
Unknown	00:1F:45:80:D5:DB	11: (2462)	-33
Unknown	00:1F:45:80:D5:DD	11: (2462)	-32
Unknown	20:B3:99:43:54:18	11: (2462)	-66
Unknown	20:B3:99:43:54:19	11: (2462)	-66
Unknown	20:B3:99:43:54:1B	11: (2462)	-66
Unknown	20:B3:99:9D:8E:78	11: (2462)	-69
Unknown	20:B3:99:9D:8E:79	11: (2462)	-69
Unknown	20:B3:99:BB:11:08	11: (2462)	-69
Unknown	20:B3:99:BB:11:09	11: (2462)	-63
Unknown	20:B3:99:BB:11:0A	11: (2462)	-63
Unknown	20:B3:99:D8:41:38	11: (2462)	-61
Unknown	20:B3:99:E5:25:B8	11: (2462)	-84
Unknown	20:B3:99:E9:04:F8	11: (2462)	-75
Unknown	20:C9:D0:20:D0:A1	11: (2462)	-79
Unknown	00:0D:0B:59:79:18	9: (2452)	-56

Data as of Feb 24, 2015 04:58:31 am

AP Performance by Radio Report

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.
- 2 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	Chnl Util (%)				RSSI (dBm)				SNR (dB)				Packet Retransmissions (pps)			
		Peak		Avg	Cur	Peak		Avg	Cur	Peak		Avg	Cur	Peak		Avg	Cur
		Prev	Cur			Prev	Cur			Prev	Cur			Prev	Cur		
AP3715_12b269465000000	a/n	0	0	0	0	0	0	-18	-3	0	94	78	92	0	2	0	0
AP3715_12b269465000000	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

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.

- 2 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																						
			Peak		Avg		Bytes Per Second				Packets Per Second				Bytes Per Second				Packets Per Second																		
			Prev	Cur	Prev	Cur	Prev	Cur	Prev	Cur	Prev	Cur	Prev	Cur	Prev	Cur	Prev	Cur																			
13310613085D0000	a	LAB6162	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	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	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

- 1 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	5	0	1	0	0	0	0	0	0	0

Data as of Mar 16, 2015 10:07:16 am

Viewing Active Clients

- From the top menu, click **Reports**. The **Available AP Reports** screen displays.

- 2 In the left pane, click **Clients**. The **Available Active Clients Reports** screen displays.

- 3 Under Available Active Clients Reports, click **By AP**. The **Active Clients by Wireless APs** display opens in a new browser window.

- The green lock icon in the first column indicates that the client is authenticated.
- The RSS (received signal strength) of a client is the average of the transmitted and received RSS on hardware platforms where both values are available.

- 4 Under Available Active Clients Reports, click **By VNS**. The **Active Clients by VNS** display opens in a new browser window.

lab-422-g - Reports - Active Clients by VNS No refresh Refresh every 30 secs Apply

Users

CNL-422-2-12-wds (CNL-422-2-12-wdsChildsWlans-ssid)

VNS	Client IP	Client MAC	AP	BSS MAC	SSID	Auth. / Priv.	Radio	Protocol ¹	RSS (dbm)	User	Time Conn.	Roamed	Role	Def. Ac
<input type="checkbox"/>	10.219.46.102	IntelCorpo_E6:CC:34:24:77:03:E6:CC:34	C4110 - ap2 - AP3620	00:1A:E8:14:2A:39	CNL-422-2-12-wdsChildsWlans-ssid	EAP / WPA	2	g	-42	tester1	5:07:22	No	CNL-422-2-12-wds-default	Cl 42 12
Traffic Summary											1			

Active Users: 1
Auth Users: 1
Non-Auth Users: 0

Search Client by user name Search

Data as of Mar 03, 2014 11:17:17 am Select All Deselect All Selected clients: Add to Blacklist Disassociate Show OUI Refresh Export Close

- 5 Under Available Active Clients Reports, click **All Active Clients**. The **All Active Clients** display opens in a new browser window.

lab-422-g - Reports - All Active Clients No refresh Refresh every 30 secs Apply

Client IP	Client MAC	AP	BSS MAC	SSID	Auth. / Priv.	Radio	Protocol ¹	RSS (dbm)	User	Time Conn.	Roamed	Role	Default Action	PVID	Avg.Rate(Mbps) Sent/Rec'd	Packets Sent/Rec'd	
<input type="checkbox"/>	10.219.46.102	IntelCorpo_E6:CC:34:24:77:03:E6:CC:34	C4110 - ap2 - AP3620	00:1A:E8:14:2A:39	CNL-422-2-12-wdsChildsWlans-ssid	EAP / WPA	2	g	-43	tester1	5:09:43	No	CNL-422-2-12-wds-default	CNL-422-2-12-wds-untagged	54/18	54333/5172	
Traffic Summary																1	54333/5172

Active Users: 1
Auth Users: 1
Non-Auth Users: 0

Search Client by user name Search

Data as of Mar 03, 2014 11:19:38 am Select All Deselect All Selected clients: Add to Blacklist Disassociate Show OUI Refresh Export Close

Viewing Role Filter Statistics

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.

- 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 left sidebar lists various categories: '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 sub-sections: '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 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.

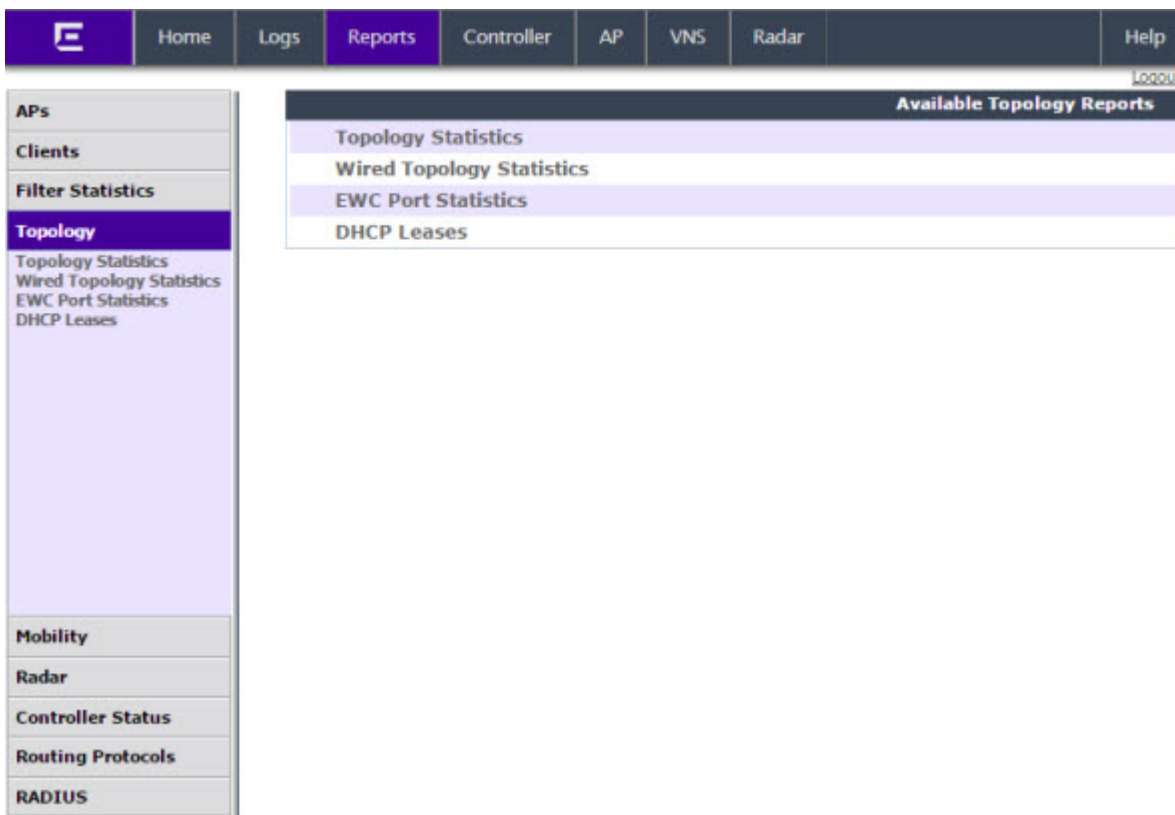
Wired Topology Statistics — Displays statistics for each topology including total packets sent and received.

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 DHCP addresses for your needs and whether the lease times are too long.

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.

- 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 30 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.

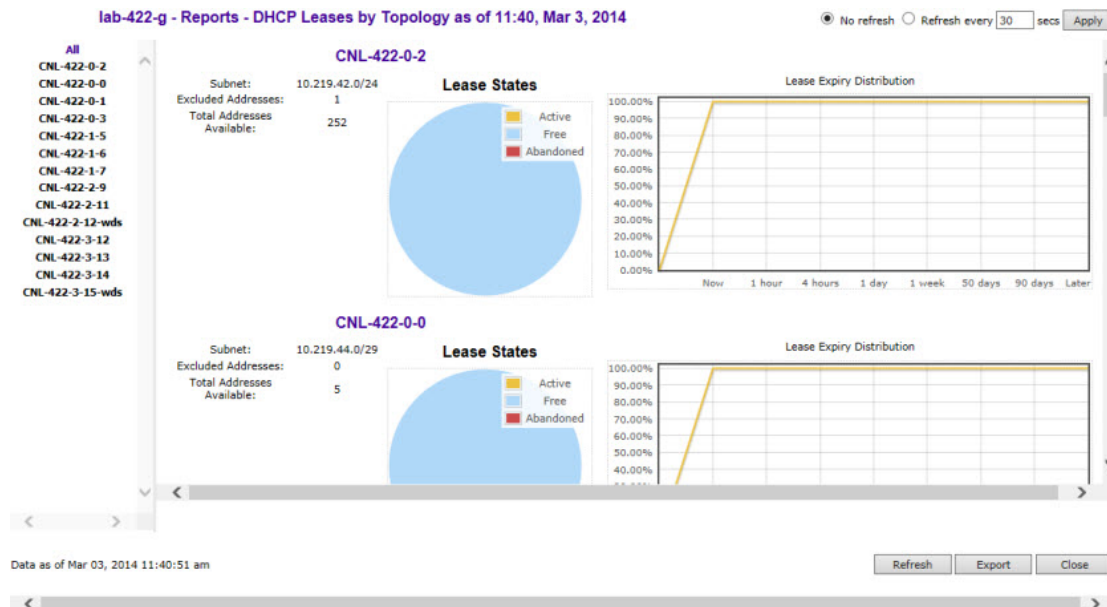
lab-422-g - Reports - Wireless Controller Port Statistics No refresh Refresh every 30 secs

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

When a controller has been configured as a mobility manager, additional displays appear as options in the left pane:

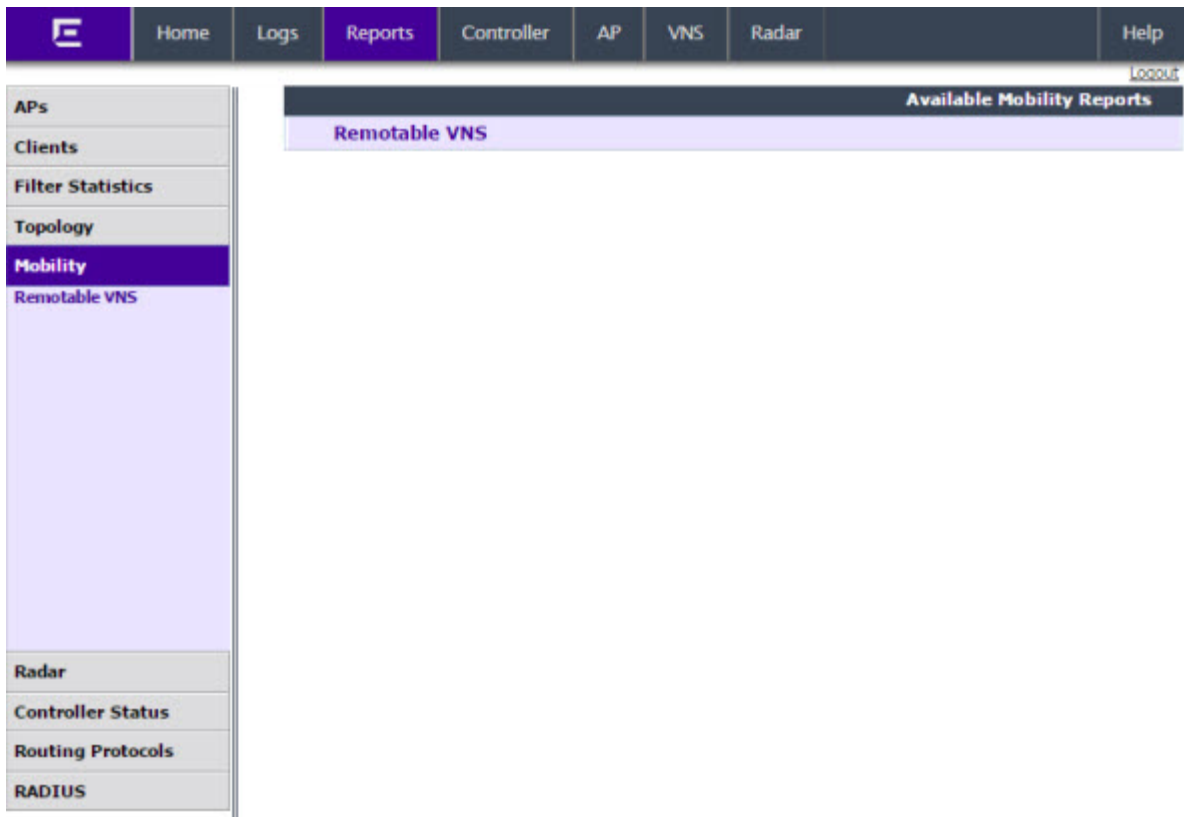
- **Client Location in Mobility Zone** — Displays the active wireless clients and their status.

- **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 Displays:

- 1 From the top menu, click **Reports**. The **Available AP Reports** screen displays.
- 2 In the left pane, click **Mobility**.
- 3 Click the appropriate mobility manager display:
 - Client Location in Mobility Zone
 - Backup Manager Mobility Tunnel Matrix
 - Remotable VNS

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

C4110-NAM - Reports - Client Location in Mobility Zone No refresh Refresh every 30 secs

Sort by: Home Wireless Controller

Search Client by user name Total mobility clients: 2

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

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.

Backup Manager Mobility Tunnel Matrix

C4110-NAM - Reports - Primary Manager Mobility Tunnel Matrix No refresh Refresh every 30 secs

Mobility Summary: Active mobility clients: 2 Data tunnels: 3 Control tunnels: 0 No tunnels: 0

Home	Foreign		
	C4110-NAM (M) (10.100.1.1)	C5110-ROW (BM) (10.100.3.1)	C25-ROW (10.200.1.1)
C4110-NAM (MID=1, M) (10.100.1.1)	home: 0 current: 0	0 clients 0:34:06	0 clients 0:33:36
C5110-ROW (MID=2, BM) (10.100.3.1)	0 clients 0:34:06	home: 0 current: 0	0 clients 0:33:38
C25-ROW (MID=3) (10.200.1.1)	0 clients 0:33:36	0 clients 0:33:38	home: 2 current: 2

- 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 it is explicitly removed by the administrator from the Mobility permission list. If a particular link between controllers, or the controller is down, the corresponding matrix connections are identified in red color 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.

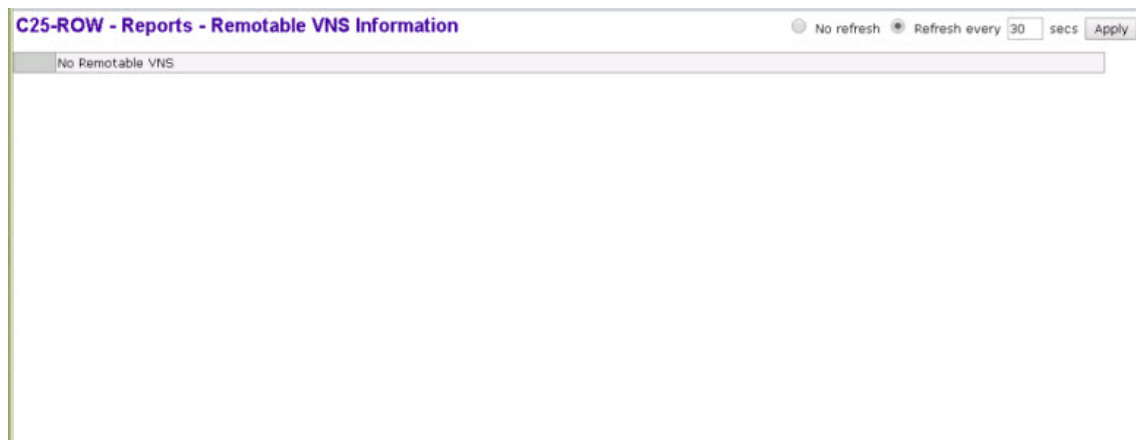
The Active Clients by AP report on each controller will show both the loading of local and foreign users (users roamed from other controllers) that are taking resources on the AP.



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



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**. The **Available AP Reports** screen displays.
- 2 In the left pane, click **Controller Status**. The **Available Controller Status Reports** screen displays.

The screenshot displays a web-based network management interface. At the top, a navigation bar contains the following items: Home, Logs, Reports (highlighted in purple), Controller, AP, VNS, Radar, and Help. A 'Logout' link is visible in the top right corner. On the left side, a vertical sidebar menu lists various categories: APs, Clients, Filter Statistics, Topology, Mobility, Radar, Controller Status (highlighted in purple), External Connections Status, System Information, Manufacturing Information, Routing Protocols, and RADIUS. The main content area on the right is titled 'Available Controller Status Reports' and contains three sub-sections: External Connections Statistics, System Information, and Manufacturing Information, each with a light purple header bar.

- 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**. The **Available AP Reports** screen displays.
- 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  1979744  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: 5640 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
  6B 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**. The **Available AP Reports** screen displays.
- 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 Identifi Wireless 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**. The **Available AP Reports** screen displays.

- 2 In the left pane, click **Routing Protocols**. The **Available Routing Protocols 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 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 is titled 'Available Routing Protocols Reports' and contains a list of three items: 'Forwarding Table', 'OSPF Neighbor', and '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**. The **Available AP Reports** screen displays.
- 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 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 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:

- On the report screen, click **Export**. A Windows **File Download** dialog is displayed.
- 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.

- 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.
- 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 Identifi Wireless 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.

- From the top menu, click **Reports**. The **Available AP Reports** screen displays.

- 2 In the left pane, click **RADIUS**. The **Available RADIUS Reports** screen displays.

The screenshot shows a web application interface. At the top is a navigation bar with tabs: Home, Logs, Reports (selected), Controller, AP, VNS, Radar, and Help. A [Logout](#) link is visible in the top right corner. On the left is a vertical sidebar menu with the following items: APs, Clients, Filter Statistics, Topology, Mobility, Radar, Controller Status, Routing Protocols, **RADIUS** (highlighted), and a sub-menu for RADIUS containing RADIUS Statistics by VNS and Access-Reject Messages. The main content area is titled "Available RADIUS Reports" and contains two report options: "RADIUS Statistics by VNS" and "Access-Reject Messages".

- 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

- 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

- 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 258.

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 132: 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 132: 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 IdentifiFi Wireless *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**. The **Wireless Controller Configuration** screen displays.
- 2 In the left pane, click **Administration** > **Software Maintenance**. The **Software Maintenance** screen displays.
- 3 Click the **Backup** tab.

The screenshot shows the 'Software Maintenance' screen with the 'Backup' tab selected. The interface includes a top navigation bar with 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Radar', and 'Help'. A left sidebar lists 'Administration' options: Availability, Flash, Host Attributes, Installation Wizard, Login Management, Software Maintenance (selected), System Maintenance, and Web Settings. Below the sidebar are sections for 'Logs', 'Network', and 'Services'. The main content area is divided into several sections:

- Available Backups:** A large empty box with 'Details' and 'Delete' buttons below it.
- Copy Selected Backup to:** Radio buttons for 'Remote' (selected) and 'Flash'. Below are input fields for Protocol (FTP), Server, User ID, Password, Confirm, Directory, and Filename, with a 'Copy' button.
- Backup:** A dropdown menu for 'Select what to backup:' set to 'Config's, CDRs, Logs and Audit', and a 'Backup to:' dropdown set to 'Local'. A 'Backup Now' button is present.
- Schedule Backups:** Fields for 'Next backup:', 'Schedule:', 'Send to:', and 'Backup of:' all showing 'Schedule backup not configured'. A 'Schedule Backups...' button is at the bottom right.
- Disk space left for Backup/Restore:** 25335 MB.

- 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.

The screenshot shows a 'Software Maintenance' window with a title bar containing a question mark and a close button. The window content displays the following text:

Please wait while performing backup of [cdrs] ...
 Result of backup:
 SUCCESS: Backup/Export complete: lab-422-g.03032014.121027

A 'Close' button is located at the bottom right of the window.

- 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.

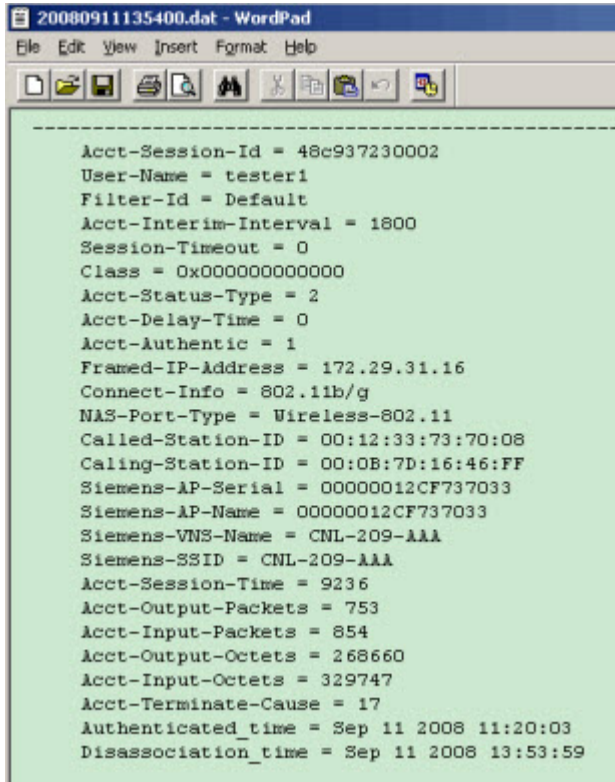
- To upload a backup to a Remote, in the **Copy Selected Backup > to** section, select **Remote**, then do the following:
 - **Protocol** — Select the file transfer protocol you want to use to upload the backup file, SCP or FTP.
 - **Server** — Type the IP address of the server where the backup will 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.
- 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.
 - In the **Copy Selected Backup to** section, click **Copy**. The .zip file is uploaded on to the server.
 - Unzip the file. The two CDR files — **.work** and **.dat** — are visible on the server.

10 To view CDRs, download the files.

A screenshot of a Windows WordPad application window. The title bar reads "20080911135400.dat - WordPad". The menu bar includes "File", "Edit", "View", "Insert", "Format", and "Help". The toolbar contains icons for file operations like Open, Save, Print, and Edit. The main text area displays a list of key-value pairs for a data record, separated by a dashed line at the top. The text is as follows:

```
-----  
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 59: Sample .dat File

18 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.
- Add a selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the AP.
- Backup and restore the controller database. For more information, see the Extreme Networks *IdentiFi Wireless Maintenance Guide*.

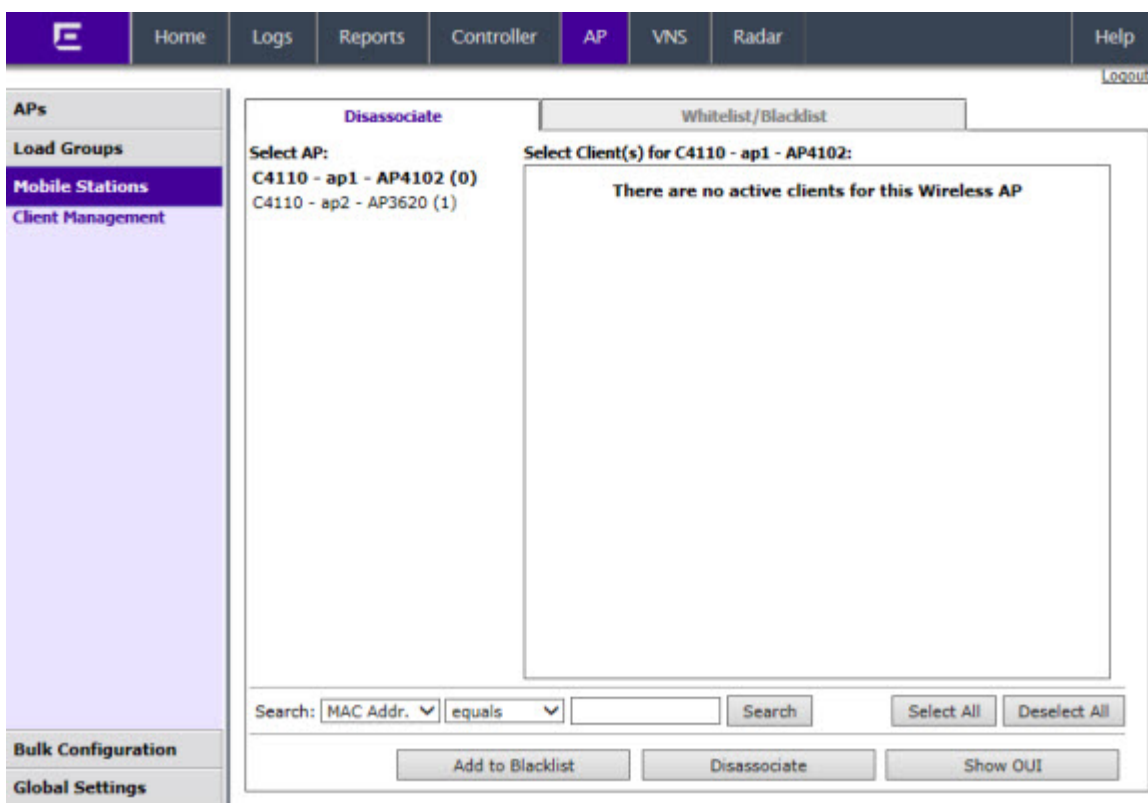
Disassociating a Client

In addition to the following procedure below, you can also disassociate wireless users directly from the Active Clients by VNS screen. For more information, see [Working with Reports and Statistics](#) on page 504.

To Disassociate a Wireless Device Client:

- 1 From the top menu, click **AP**. The **AP** screen displays.

- In the left pane, click **Mobile Stations** > **Client Management**. The **Disassociate** tab is displayed.



- In the **Select AP** list, click the AP that is connected to the client that you want to disassociate.
- In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate.
- To search for a client by MAC Address, IP Address or User ID, select the search parameters from the drop-down lists, type a search string in the **Search** box, and click **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.
- Click **Disassociate**. The client's session terminates immediately.

Blacklisting a Client

The **Whitelist/Blacklist** tab displays the current list of MAC addresses that are not allowed to associate. A client is added to the blacklist by selecting it from a list of associated APs or by typing its MAC address.

To blacklist a wireless device client:

- From the top menu, click **AP**. The **AP** screen displays.

- In the left pane, click **Mobile Stations > Client Management**.

The **Disassociate** tab is displayed.

The screenshot shows the 'AP' configuration page with the 'Disassociate' tab selected. The left sidebar contains a tree view with 'Mobile Stations' and 'Client Management' highlighted. The main content area is divided into two sections: 'Select AP:' and 'Select Client(s) for C4110 - ap1 - AP4102:'. The 'Select AP:' section lists two APs: 'C4110 - ap1 - AP4102 (0)' and 'C4110 - ap2 - AP3620 (1)'. The 'Select Client(s)' section is currently empty, displaying the message 'There are no active clients for this Wireless AP'. At the bottom, there is a search bar with dropdown menus for 'MAC Addr.' and 'equals', a 'Search' button, and 'Select All' and 'Deselect All' buttons. Below the search bar are three buttons: 'Add to Blacklist', 'Disassociate', and 'Show OUI'.

- In the **Select AP** list, click the AP that is connected to the client that you want to blacklist.
- In the **Select Client(s)** list, select the checkbox next to the client you want to blacklist, if applicable.

Note



You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the **Search** box and clicking Search. You can also use the Select All or **Clear All** buttons to help you select multiple clients.

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

Blacklisting a Client Using its MAC Address

To blacklist a wireless device client using its MAC address:

- From the top menu, click **AP**. The **AP** screen displays.
- In the left pane, click **Mobile Stations > Client Management**. The **Disassociate** tab is displayed.

- 3 Click the **Whitelist/Blacklist** tab.

- 4 To add a new MAC address to the blacklist, in the **MAC Address** box type the client's MAC address.
- 5 Click **Add**. The client is displayed in the **MAC Addresses** list.



Note

You can use the **Select All** or **Clear All** buttons to help you select multiple clients.

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

Clearing a Blacklisted Address

To clear an address from the blacklist:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Mobile Stations** > **Client Management**. The **Disassociate** tab is displayed.
- 3 Click the **Whitelist/Blacklist** tab.
- 4 To clear an address from the blacklist, select the corresponding checkbox in the **MAC Addresses** list.
- 5 Click **Remove Selected**. The selected client is removed from the list.



Note

You can use the **Select All** or **Clear All** buttons to help you select multiple clients.

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

Selecting OUI/IABs

To select OUI/IABs:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Mobile Stations > Client Management**. The **Disassociate** tab is displayed.
- 3 Click the **Whitelist/Blacklist** tab.
- 4 To select an OUI (Organizationally Unique Identifier)/IAB (Individual Address Block) from the list of company's, click **Select OUI/IAB**. The Configure OIU/IAB dialog displays.



- 5 Enter a specific company name and click **Search company**.
- 6 Select the corresponding checkbox in the **OUI/IAB** list.



Note

You can use the **Select All** or **Deselect All** buttons to help you select or deselect multiple clients.

- 7 Click **OK**.

Importing a List of MAC Addresses for the Blacklist

To import a list of MAC addresses for the blacklist:

- 1 From the top menu, click **AP**. The **AP** is displayed.
- 2 In the left pane, click **Mobile Stations > Client Management**. The **Disassociate** tab is displayed.
- 3 Click the **Whitelist/Blacklist** tab.
- 4 Click **Browse** and navigate to the file of MAC addresses you want to import and add to the blacklist.
- 5 Select the file, and then click **Import**. The list of MAC addresses is imported.

Exporting a List of MAC Addresses for the Blacklist

To export a list of MAC addresses for the blacklist:

- 1 From the top menu, click **AP**. The **AP** screen displays.
- 2 In the left pane, click **Mobile Stations > Client Management**. The **Disassociate** tab is displayed.
- 3 Click the **Whitelist/Blacklist** tab.

- 4 Click **Export**. The saved blacklist file is exported.
- 5 To export the current blacklist, use the browser's Save option to save the file as a text (.txt) file. We recommend using a descriptive file name.

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

When adding or modifying a user, note the following password character constraints:

- Allowed characters include A-Z a-z 0-9 ~!@#\$%^&*()_+|=~\{}[];<>?.,
- Characters not allowed include / ` ' " : and space is not valid.

To Add a Controller Administrator to a Login Group:

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

- 2 In the left pane, click **Administration** > **Login Management**. The **Local Authentication** tab is displayed.

- 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 544.
- 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.
To Modify a Controller Administrator's Password:
- 8 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
- 9 In the left pane, click **Administration** > **Login Management**. The **Local Authentication** tab is displayed.

- 10 Click the user whose password you want to modify.
- 11 In the **Password** box, type the new password for the user.
- 12 Under **Confirm Password** re-type the new password.
- 13 To change the password, click **Change Password**.
To Remove a Controller Administrator:
 - 14 From the top menu, click **Controller**. The **Wireless Controller Configuration** screen displays.
 - 15 In the left pane, click **Administration** > **Login Management**. The **Local Authentication** tab is displayed.
 - 16 Click the user you want to remove.
 - 17 Click **Remove user**. The user is removed from the list.

19 Logs, Traces, Audits and DHCP Messages

IdentifiFi Wireless 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

IdentifiFi Wireless Appliance Messages

The IdentifiFi Wireless 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 IdentifiFi Wireless *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 DHCP 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**. The **Logs & Traces** screen displays.

- 2 Click **EWC Events**. The log screen displays and the events are displayed in chronological order.

Timestamp	Type	Component	Log Message
03/03/14 05:57:11	Critical	CLI	USER GENERATED EVENT: Critical Logs During Smoke Test - lab-422-g-1403030332
03/03/14 04:18:53	Critical	CLI	USER GENERATED EVENT: Critical Logs During Smoke Test - lab-422-g-1403030332

- 3 To sort the events by Timestamp, Type, or Component, click the appropriate column heading.
- 4 To filter the events by severity, Critical, Major, Minor, Info, and All, click the appropriate log severity.
- 5 To refresh the log screen, click **Refresh**.
- 6 To export the log screen, click **Export**. The **File Download** dialog is displayed.
- 7 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:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.

- 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	Room	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

First Previous 1 Next Last

[†] 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**. The **Logs & Traces** screen displays.
- 2 Click **AP: Logs**. The Wireless AP log screen displays and the events are displayed in chronological order.

The screenshot shows the 'AP: Logs' screen. At the top, there is a navigation bar with 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'Raclar', and 'Help'. Below this is a breadcrumb trail: 'EWC: Events | Station Events | Restore/Import | S/W Upgrade • AP: Logs | Traces • Audit: UI • Services: DHCP | NTP | Login'. A severity filter is set to 'All'. The main table has columns: 'Wireless AP', 'EWC time', 'Sev', and 'AP-time/up-time : Log Messages'. The table contains several rows of log entries, including noise threshold exceedances and successful secure tunnel connections. At the bottom, there are navigation buttons: 'First', 'Previous', 'Next', 'Last', 'Export', and 'Refresh'. A status bar at the bottom left indicates '94 messages'.

Wireless AP	EWC time	Sev	AP-time/up-time : Log Messages
	10/21/14 11:46:58	Info	10/21/14 15:46:57: DCS Measured Noise -87dBm Exceeded Threshold of -95dBm on chann. 2472Mhz
	10/21/14 11:45:58	Info	10/21/14 15:45:57: DCS Measured Noise -91dBm Exceeded Threshold of -95dBm on chann. 2472Mhz
	10/20/14 15:00:24	Info	26 sec in cycle 6: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:59:00	Info	27 sec in cycle 5: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:57:12	Info	27 sec in cycle 4: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:55:37	Info	26 sec in cycle 3: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:53:38	Info	27 sec in cycle 2: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:51:13	Info	27 sec in cycle 1: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:47:30	Info	26 sec in cycle 1: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:47:30	Critical	10/20/14 18:46:44: AccessPoint Rebooting due to: Software Image Upgrade
	10/20/14 14:47:30	Major	10/20/14 18:46:42: AccessPoint software upgrade done with image AP3805/AP3805-09.15.01.0095.img.
	10/20/14 14:44:40	Info	26 sec in cycle 14: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.
	10/20/14 14:42:00	Info	27 sec in cycle 13: The AP 10.200.0.190 has successfully connected to AC 10.200.1.1 using secure tunnel.

- 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**. The **Logs & Traces** screen displays.
- 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**. The **Logs & Traces** screen displays.
- 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.

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

To Generate a Tech Support File:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.
- 2 Ensure that **EWC:Events** is selected.

- Click the **Tech Support** button at the bottom of the page. The **Generate Tech Support File** screen displays.

Extreme networks Tech Support Progress

Select the required parameters for the Tech Support File.

Wireless Controller
 Wireless AP
 Log
 All
 No Stats

Generate New Tech Support File
 Download Last Tech Support File
 List All Tech Support Files
 Close

- 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.
- Click **Generate New Tech Support File**. A warning message is displayed informing you that this operation may temporarily affect system performance.
- Click **OK** to continue. The tech support file generation status is displayed.
- When the file generation has completed, click **Close**.
To Download the Last Generated Tech Support File:
- From the top menu, click **Logs**. The **Logs & Traces** screen displays.
- Ensure that the **EWC** tab is selected.
- Click the **Tech Support** button at the bottom of the page. The **Generate Tech Support File** screen displays.
- Click **Download Last Tech Support File**. The **File Download** dialog is displayed.
- Click **Save**. The **Save as** window is displayed.
- Navigate to the location you want to save the generated tech support file, and then click **Save**.
To Delete a Tech Support File:
- From the top menu, click **Logs**. The **Logs & Traces** screen displays.
- 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**. The **Logs & Traces** screen displays.
- 2 Click **AP: Traces**. The Wireless AP trace screen displays.

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 the Extreme Networks IdentifiFi Wireless Convergence Software *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.

- 3 In the **Wireless AP** list, click the Wireless AP whose trace messages you want to view.

- 4 In the **Tracing** section, do the following:
 - a **Collect traces for: Configurations** – Select to collect trace configuration information.
 - **Start/Stop Tracing** – Click to start or stop the collection of traces.
 - **Retrieve Traces** – Click to view the available configuration traces in the Trace Log Output section.
 - b **Collect traces for: Debug info** – Select to collect trace debug information.
 - **Start/Stop Tracing** – Click to start or stop the collection of traces.
 - **Retrieve Traces** – Click to view the available debug traces in the Trace Log Output section.
 - c **Collect traces for: Reports** – Select to view available crash files.
 - **Retrieve Traces** – Click to view available crash files in the Trace Log Output section.
 - **Delete all crash reports** – Click to delete all crash reports.
- 5 To refresh the trace screen, click **Refresh**.
- 6 To export and view the Wireless AP trace screen in HTML format, click **Export**.

Viewing the Wireless 802.11n and 802.11ac AP Traces

Wireless 802.11n and 802.11ac AP traces are combined into a single .tar.gz file and can only be viewed by saving the .tar.gz file to a directory on your computer.

To View Wireless 802.11n and 802.11ac AP Traces:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.
- 2 Click the **AP Traces** tab. The Wireless AP trace screen displays.
- 3 In the **Active 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.gz file.
- 6 To view the file, unzip the .tar.gz file.

Viewing Audit Messages

To View Audit Messages:

- 1 From the top menu, click **Logs**. The **Logs & Traces** screen displays.

- 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

- To sort the events by **Timestamp, User, Section, or Page**, click the appropriate column heading.
- To refresh the audit screen, click **Refresh**.
- To export the audit screen, click **Export**. The **File Download** dialog is displayed.
- 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 DHCP Messages:

- 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

- 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 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**.

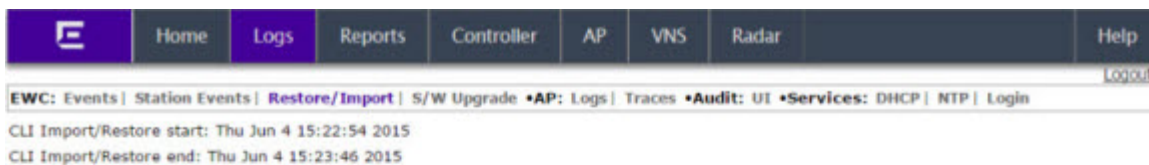
Viewing Configuration Restore/Import Messages

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**.

20 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 GuestPortal Ticket Page
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 369.

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 549.

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

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 570.
- 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 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 "Print Ticket for Selected Account" button. 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 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 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**. 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 Portal 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:

	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 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 edit.
- 3 In the **Account Management** section, click **Edit Selected Accounts**. The **Edit Guest User** screen displays.
- 4 Edit the guest account accordingly. For more information on guest account properties, see [Adding New Guest Accounts](#) on page 567.
- 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.

To Remove 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**. 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:

	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:** Contains buttons for "Add Guest Account", "Edit Selected Accounts", and "Remove Selected Accounts".
- Account Enable/Disable:** Contains buttons for "Enable Selected Accounts" and "Disable Selected Accounts".
- File Management:** Contains buttons for "Import Guest File" and "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 133: 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)

To Export a Guest File

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.

Search
User Name:

	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"/>

Account Management:

Account Enable/Disable:

File Management:

- 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.

To Import a Guest File

- 7 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.

Search
User Name:

	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"/>

Account Management:

Account Enable/Disable:

File Management:

- 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 GuestPortal Ticket Page](#) on page 577.

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.

Search
 User Name:

	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:

- 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 648.

Working with the GuestPortal Ticket Page

Working with the GuestPortal ticket page can include activating a GuestPortal ticket page, uploading a customized GuestPortal ticket page to the controller, and deleting 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.

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 648.

Activating a GuestPortal Ticket Page

To Activate a GuestPortal Ticket Page:

- 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 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 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.

- 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' page. The top navigation bar includes 'Home', 'Logs', 'Reports', 'Controller' (selected), 'AP', 'VNS', 'Radar', and 'Help'. A 'Logout' link is in the top right. The left sidebar lists 'Administration' (selected) with sub-items: Availability, Flash, Host Attributes, Installation Wizard, Login Management, Software Maintenance, System Maintenance, and Web Settings. Below this are 'Logs', 'Network', and 'Services'. The main content area is titled 'Wireless Controller Web Management Settings' and contains:

- Web Session Timeout:** A text input field containing '1:00' with the text '(hour:minutes, or just minutes)' to its right.
- GuestPortal Manager Web Session Timeout:** A text input field containing '1:00' with the text '(hour:minutes, or just minutes)' to its right.
- Below these fields is the text 'range 1 minute to 7 days'.
- A checkbox labeled 'Show WLAN names on the Wireless AP SSID list'.
- A 'Save' button is located in the bottom right corner.

- 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.
- 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.
- Select the **Show WLAN names on the Wireless AP SSID list** checkbox to allow the names of the WLAN services to appear in the SSID list for IdentifiFi Wireless APs.
- 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 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 Summit X450 a-series switch), certain ports can be used as either copper or fiber 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 [Class of Service \(CoS\)](#) in the *ExtremeXOS 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 User Guide*.

datagram

See [packet](#).

dBm

An abbreviation for the power ratio in decibels (dB) of the measured power referenced to one milliwatt.

DCB

Data Center Bridging 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.

decapsulation

See [tunelling](#).

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 an 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 [Denial of Service Protection](#) in the *ExtremeXOS 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 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 [Understanding Fabric Modules](#) in the *BlackDiamond X 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 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, hitless failover means that designated configurations survive a change of primacy between the two MSMs with all details intact. Thus, those features run seamlessly during and after control of the system changes from one MSM 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 NetSight 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 [Understanding Management Modules](#) in the *BlackDiamond X 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 [Introduction to Rate Limiting, Rate Shaping, and Scheduling](#) in the *ExtremeXOS 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 [Introduction to Rate Limiting, Rate Shaping, and Scheduling](#) in the *ExtremeXOS 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. At Extreme Networks, SSL is bundled with the SSH software module, which must be downloaded separately. SSL used for other applications than SSH, [CNA](#) at Extreme Networks for example.

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.

TRILL

Transparent Interconnection of Lots of Links. TRILL allows for improved scaling of data center servers and virtual machine interconnections by combining bridged networks with network topology control and routing management.

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).

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.

B Regulatory Information

IdentifiFi Wireless APs 37XX and 38XX IdentifiFi Wireless APs 26XX and 36XX



Warning

Warnings identify essential information. Ignoring a warning can lead to problems with the application.

This appendix provides regulatory information only for the Extreme Networks IdentifiFi Wireless AP models 2610/20 and 3610/20.



Note

Throughout this appendix, the term 'IdentifiFi Wireless AP' refers to AP models (AP26XX series, and AP36XX series). Specific AP models are only identified in this appendix where it is necessary to do so.



Note

For technical specifications and certification information for a specific IdentifiFi Wireless Outdoor AP see the IdentifiFi Wireless Outdoor AP Installation Guide.

Configuration of the IdentifiFi Wireless 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 IdentifiFi Wireless 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 IdentifiFi Wireless 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 this guide.



Note

The IdentifiFi Wireless 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.

IdentifiFi Wireless APs 37XX and 38XX

For regulatory information for the Extreme Networks IdentifiFi Wireless AP models 37xx and 38xx, refer to the appropriate AP Installation Guide.

IdentiFi Wireless APs 26XX and 36XX

This device is suitable for use in environmental air space in accordance with Section 300.22.C of the National Electrical Code, and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1.

Wi-Fi Certification

The AP26XX is Wi-Fi certified for operation in accordance with IEEE 802.11a/b/g. The AP2610/20 IdentiFi Wireless APs with internal and external antennas are designed and intended to be used indoors.

The AP36XX is Wi-Fi certified for operation in accordance with IEEE 802.11a/b/g/n. The AP36XX IdentiFi Wireless APs with internal and external antennas are designed and intended to be used indoors.

Table 134: IdentiFi Wireless AP Wi-Fi Certification ID

IdentiFi Wireless AP model	Wi-Fi certification ID
AP2605	WFA7482
AP2610	WFA7432
AP2620	WFA7387
AP2650	WFA7386
AP2660	WFA7431
AP3605	WFA9173
AP3610	WFA6025
AP3620	WFA5917



Note

Operation in the European Community and rest of the world may be dependant on securing local licenses, certifications, and regulatory approvals.

AP2620 External Antenna AP

Approved External Antennas

The AP2620 external antenna APs can also be used with optional certified external antennas:

- The external antennas on the AP2620 must be identical.
- Any unused antenna ports must be terminated when an external antenna is used with the AP2620.

Antenna Diversity

There are some limitations for using different antennas and Tx/Rx diversity:

- If Alternate antenna diversity is used for Tx or Rx, then the same antenna model must be used as left and right antennas. In addition, if cables are used to connect external antennas, the cables must be of the same length and similar attenuation. If these rules are not respected, antenna diversity will not function properly and there will be degradation in the link budget in both directions.

- You can choose to install only one antenna provided that both Tx and Rx diversity are configured to use that antenna and only that antenna. You can choose to install one antenna for 11b/g band and one antenna for 11a band, provided that the antenna diversity is configured appropriately on both radios.

AP3620 External Antenna AP

Approved External Antennas

The AP3620 external antenna APs can also be used with optional certified external antennas:

- Any unused antenna ports must be terminated when an external antenna is used with the AP3620.

United States

FCC Declaration of Conformity Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential and business environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause harmful interference, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment or devices.
- Connect the equipment to an outlet other than the receiver's.
- Consult a dealer or an experienced radio/TV technician for suggestions.

USA Conformance Standards

This equipment meets the following conformance standards:

Safety

- UL 60950-1
- UL 2043 Plenum Rated as part of UL 60950-1. Suitable for use in environmental air space in accordance with Section 300.22.C of the National Electrical Code.

EMC

- FCC CFR 47 Part 15, Class B

Radio Transceiver

- CFR 47 Part 15.247, Subpart C
- CFR 47 Part 15.407, Subpart E

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

**Warning**

The IdentifiFi Wireless APs must be installed and used in strict accordance with the manufacturer's instructions as described in this guide and related documentation for the device to which the IdentifiFi Wireless AP is connected. Any other installation or use of the product violates FCC Part 15 regulations. Operation of the IdentifiFi Wireless AP is restricted for indoor use only, specifically in the UNII 5.15 - 5.25 GHz band in accordance with 47 CFR 15.407(e). This Part 15 radio device operates on a non-interference basis with other devices operating at the same frequency when using antennas provided or other Extreme Networks certified antennas. Any changes or modification to the product not expressly approved by Extreme Networks could void the user's authority to operate this device. For the product available in the USA market, only channels 1 to 11 can be operated. Selection of other channels in the 2.4 GHz band is not possible.

FCC RF Radiation Exposure Statement

The IdentifiFi Wireless AP complies with FCC RF radiated exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This device has been tested and has demonstrated compliance when simultaneously operated in the 2.4 GHz and 5 GHz frequency ranges. This device must not be co-located or operated in conjunction with any other antenna or transmitter.

**Caution**

The radiated output power of the IdentifiFi Wireless AP is below the FCC radio frequency exposure limits as specified in "Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields" (OET Bullet 65, Supplement C). This equipment should be installed and operated with a minimum distance of 25 cm between the radiator and your body or other co-located operating antennas. For all external antennas, the minimum separation distance should be 25 cm. However, when using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 42cm.

External Antennas

The AP2620/AP3620 external antenna APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see [AP2620 Approved External Antennas](#) on page 643.

RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

For all external antennas, the minimum separation distance should be 25 cm. However, when using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 42cm.

Canada*Industry Canada Compliance Statement*

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le Industrie Canada.

This device complies with Part 15 of the FCC Rules and Canadian Standard RSS-210. Operation is subject to the following conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.
- This Class B digital apparatus complies with Canadian ICES-003.
- Operation in the 5150-5250 MHz band is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
- Please note that high power radars are allocated as primary users (meaning they have priority) and can cause interference in the 5250-5350 MHz and 5470-5725 MHz bands of LE-LAN devices.
- For the product available in the Canadian market, only channels 1 to 11 can be operated. Selection of other channels in the 2.4 GHz band is not possible.

Canada Conformance Standards

This equipment meets the following conformance standards:

Safety

- C22.2 No.60950-1-03
- UL 2043 Plenum Rated as part of UL 60950-1. Suitable for use in environmental air space in accordance with Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1

EMC

- ICES-003, Class B

Radio Transceiver

- RSS-210 (2.4 GHz and 5 GHz)

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

External Antennas

The AP2620/AP3620 external antenna APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see [AP2620 Approved External Antennas](#) on page 643.

RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

For all external antennas, the minimum separation distance should be 25 cm. However, when using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 42cm.

European Community

The IdentifiFi Wireless APs are designed for use in the European Union and other countries with similar regulatory restrictions where the end user or installer is allowed to configure the IdentifiFi Wireless AP for operation by entry of a country code relative to a specific country. Upon connection to the controller, the software will prompt the user to select a country code. After the country code is selected, the controller will set up the IdentifiFi Wireless AP with the proper frequencies and power outputs for that country code.

Although outdoor use may be allowed and may be restricted to certain frequencies and/or may require a license for operation, the IdentifiFi Wireless AP is intended for indoor use and must be installed in a proper indoor location. Use the installation utility provided with the controller software to ensure proper set-up in accordance with all European spectrum usage rules. Contact local Authority for procedure to follow and regulatory information. For more details on legal combinations of frequencies, power levels and antennas, contact Extreme Networks.

Declaration of Conformity with R&TTE Directive of the European Union 1999/5/EC

The following symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).



Declaration of Conformity in Languages of the European Community

English	Hereby, Extreme Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Extreme Networks vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Extreme Networks dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart Extreme Networks dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente Extreme Networks déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, Extreme Networks déclare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
Swedish	Härmed intygar Extreme Networks att denna Radio LAN device står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede Extreme Networks erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erkläre Extreme Networks die Übereinstimmung des "WLAN Wireless Controller bzw. Access Points" mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG.
Greek	Extreme Networks Radio LAN device 1999/5/ .
Icelandic	Extreme Networks lýsir her með yfir að thessi bunadur, Radio LAN device, uppfyllir allar grunnkröfur, sem gerðar eru í R&TTE tilskipun ESB nr 1999/5/EC.
Italian	Con la presente Extreme Networks dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Extreme Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Portuguese	Extreme Networks declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hawnhekk, Extreme Networks, jiddikjara li dan Radio LAN device jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.

New Member States Requirements of Declaration of Conformity

Estonian	Käesolevaga kinnitab Extreme Networks seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Hungary	Alulírott, Extreme Networks nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Slovak	Extreme Networks týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

Czech	Extreme Networks tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES."
Slovenian	Šiuo Extreme Networks deklaruojā, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar šo Extreme Networks deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem
Lithuanian	Extreme Networks deklaruojā, kad Radio LAN device atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".
Polish	Niniejszym, Extreme Networks, deklaruje, że Radio LAN device spełnia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

European Conformance Standards

This equipment meets the following conformance standards:

Safety

- 2006/95/EC Low Voltage Directive (LVD)
- IEC/EN 60950-1 + National Deviations

EMC (Emissions / Immunity)

- 2004/108/EC EMC Directive
- EN 55011/CISPR 11, Class B, Group 1 ISM
- EN 55022/CISPR 22, Class B
- EN 55024/CISPR 24, includes IEC/EN 61000-4-2,3,4,5,6,11
- EN 61000-3-2 and -3-3 (Harmonics and Flicker)
- EN 60601-1-2 (EMC immunity for medical equipment)
- EN 50385 (EMF)
- ETSI/EN 301 489-1 & -17

Radio Transceiver

- R&TTE Directive 1999/5/EC
- ETSI/EN 300 328 (2.4 GHz)
- ETSI/EN 301 893 (5 GHz)

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

RoHS

- European Directive 2002/95/EC

External Antennas

The AP2620/AP3620 external antenna APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see [AP2620 Approved External Antennas](#) on page 643.

RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

For all external antennas, the minimum separation distance should be 25 cm. However, when using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 42cm.

Conditions of Use in the European Community

The IdentifiFi Wireless APs with internal and external antennas are designed and intended to be used indoors. Some EU countries allow outdoor operation with limitations and restrictions, which are described in this section. It is the responsibility of the end user to ensure operation in accordance with these rules, frequencies, and transmitter power output. The IdentifiFi Wireless AP must not be operated until properly configured for the customer's geographic location.

Caution



The user or installer is responsible to ensure that the IdentifiFi Wireless AP is operated according to channel limitations, indoor / outdoor restrictions, license requirements, and within power level limits for the current country of operation. A configuration utility has been provided with the IdentifiFi Wireless Appliance to allow the end user to check the configuration and make necessary configuration changes to ensure proper operation in accordance with the spectrum usage rules for compliance with the European R&TTE directive 1999/5/EC. The IdentifiFi Wireless APs with internal and external antennas are designed to be operated only indoors within all countries of the European Community. Some countries require limited channels of operation. These restrictions are described in this section.

Caution

The IdentifiFi Wireless AP is completely configured and managed by the IdentifiFi Wireless Appliance connected to the network. Please follow the instructions in this user guide to properly configure the IdentifiFi Wireless AP. • The IdentifiFi Wireless APs require the end user or installer to ensure that they have a valid license prior to operating the IdentifiFi Wireless AP. The license contains the region and the region exposes the country codes which allow for proper configuration in conformance with European National spectrum usage laws • There is a default group of settings that each IdentifiFi Wireless AP receives when it connects to the controller. There is the ability to change these settings. The user or installer is responsible to ensure that each IdentifiFi Wireless AP is properly configured. • The software within the controller will automatically limit the allowable channels and output power determined by the selected country code. Selecting the incorrect country of operation or identifying the proper antenna used, may result in illegal operation and may cause harmful interference to other systems. • This device employs a radar detection feature required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar. • The 5 GHz Turbo Mode feature is not enabled for use on the IdentifiFi Wireless APs. • The 5150- 5350 MHz band, channels 36, 40, 44, 48, 52, 56, 60, or 64, are restricted to indoor use only. • The external antenna APs must only use antennas that are certified by Extreme Networks. • The 2.4 GHz band, channels 1 - 13, may be used for indoor or outdoor use but there may be some channel restrictions. • In Greece and Italy, the end user must apply for a license from the national spectrum authority to operate outdoors. • In France, outdoor operation is not permitted in the 2.4 GHz band.

*European Spectrum Usage Rules*

The AP configured with approved internal or external antennas can be used for indoor and outdoor transmissions throughout the European community as displayed in [Table 135: European Spectrum Usage Rules](#) on page 641. Some restrictions apply in Belgium, France, Greece, and Italy.

Table 135: European Spectrum Usage Rules

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116, 132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Austria	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Belgium	Indoor only	Indoor only	Indoor or outdoor *	Indoor or outdoor
Bulgaria	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Denmark	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Croatia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Cyprus	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Czech Rep.	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Estonia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Finland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor

Table 135: European Spectrum Usage Rules (continued)

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116, 132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
France	Indoor only	Indoor only	Indoor or outdoor	Indoor only
Germany	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Greece	Indoor only	Indoor only	Indoor (Outdoor w/ License)	Indoor (Outdoor w/ license)
Hungary	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Iceland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Ireland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Italy	Indoor only	Indoor only	Indoor or outdoor	Indoor (Outdoor w/ license)
Latvia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Liechtenstein	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Lithuania	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Luxembourg	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Netherlands	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Malta	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Norway	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Poland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Portugal	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Romania	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Slovak Rep.	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Slovenia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Spain	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Sweden	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Switzerland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Turkey	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
U.K	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor

**Note**

* Belgium requires notifying the spectrum agency if deploying > 300 meter wireless links in outdoor public areas.

Certifications of Other Countries

The IdentifiFi Wireless APs have been certified for use in various other countries. When the IdentifiFi Wireless AP is connected to the IdentifiFi Wireless Appliance, the user is prompted to select a country code. Once the correct country code is selected, the controller automatically sets up the IdentifiFi Wireless AP with the proper frequencies and power outputs for that country code.



Note

It is the responsibility of the end user to select the proper country code for the country the device will be operated within or run the risk violating local laws and regulations.

Approved External Antennas

The external antenna IdentifiFi Wireless APs can also be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

For a list of approved external antennas, see [AP2620 Approved External Antennas](#) on page 643.

Other Country Specific Compliance Standards, Approvals and Declarations

- IEC 60950-1 CB Scheme + National Deviations
- AS/NZS 60950.1 (Safety)
- AS/NZS 3548 (Emissions via EU standards – ACMA)
- AS/NZS 4288 (Radio via EU standards)
- EN 300 328 (2.4 GHz)
- EN 301 893 (5 GHz)
- EN 301 489-1 & -17 (RLAN)
- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP36XX)
- IEEE 802.3af (PoE)

AP2620 Approved External Antennas

The AP2620 can be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The optional antennas listed in [Table 136: List of FCC/IC/ETSI Approved Antennas – AP2620](#) on page 644 have been tested and approved for use with the external antenna models.

This device has been designed to operate with the optional antennas listed below, and having a maximum gain of 18 dB. Antennas not included in this list or having a gain greater than 18 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communication.

Table 136: List of FCC/IC/ETSI Approved Antennas – AP2620

Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Connector Type
WS-ANT01	outdoor	omni	4	2400-2500 5150-5900	RPSMA
WS-AO-DS05360	outdoor	omni	5	2400-2500 5150-5350	Reverse Polarity Type-N
WS-AIO-5S12060	indoor	panel	12	2400-2500 4900-5990	Reverse Polarity Type-N
WS-AI-2S03360	indoor	omni	3.5	2400-2500	RPSMA
WS-AI-DS06360	indoor	omni	5 6	2300-2700 4900-6000	RPSMA
WS-AIO-DS05120	indoor/outdoor	panel	5	2400-2500	Reverse Polarity Type-N
WS-AIO-2S07060	indoor/outdoor	panel	7.5	2300-2600 4900-6000	Reverse Polarity Type-N
WS-AIO-5S17017	indoor/outdoor	panel	17	5470-5850	Reverse Polarity Type-N
WS-AIO-2514090	indoor/outdoor	panel	14	2400-2485	Reverse Polarity Type-N
WS-AIO-5S15090	indoor/outdoor	panel	15	4900-6000	Reverse Polarity Type-N
WS-AIO-2S18018	indoor/outdoor	panel	18	2300-2500	Reverse Polarity Type-N

RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

For all external antennas, the minimum separation distance should be 25 cm. However, when using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 42cm.

AP3620 Approved External Antennas

The AP3620 can be used with certified external antennas. However, to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The optional antennas listed in [Table 137: List of FCC/IC/ETSI Approved Antennas – AP3620](#) on page 645 have been tested and approved for use with the external antenna models.

This device has been designed to operate with the optional antennas listed below, and having a maximum gain of 23 dB. Antennas not included in this list or having a gain greater than 23 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communication.

Table 137: List of FCC/IC/ETSI Approved Antennas — AP3620

Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Connector Type
WS-ANT02	indoor	omni	4	2400-2500 5150-5900	RPSMA
WS-AO-DS05360	outdoor	omni	5	2400-2500 5150-5350	Reverse Polarity Type-N
WS-AO-DI6060	outdoor	60 degree sector directional, 2 inputs	16	5150-5875	Reverse Polarity Type-N
WS-AO-5D23009	outdoor	panel, 2 inputs	23	5150-5875	Reverse Polarity Type-N
WS-AI-DT04360	indoor	omni, 3 inputs	3 4	2400-2500 4900-5990	RPSMA, 3ea.
WS-AI-DT05120	indoor	120 degree sector directional, 3 inputs	5	2300-2700 4900-6100	RPSMA

RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

For all external antennas, the minimum separation distance should be 25 cm. However, when using the WS-AO-5D23009 antenna, the minimum separation distance should be increased to 71cm. When using the WS-AIO-2S18018 antenna, the minimum separation distance should be increased to 42cm.

Certified 3rd Party Antennas

Table 138: Certified 3rd Party Antennas for Use with AP2620, AP260-1, AP3620 and AP3620-1 Models on page 645 lists the 3rd party antennas that are supported for AP2620, AP260-1, AP3620 and AP3620-1 models for ETSI and FCC. These antennas are supported only for existing customers prior to V7.11.

Table 138: Certified 3rd Party Antennas for Use with AP2620, AP260-1, AP3620 and AP3620-1 Models

AP	Regulatory	Manufacturer	Part Number	Type	Usage	Frequency	Gain	Connector
2620	FCC/IC	Cushcraft	SR2405135D	Sector, 135 Deg Single Feed	Indoor	2.4	5	N-F
2620	FCC/IC	Cushcraft	S24493DS	Omni, Dual Feed	Indoor	2.4, 5	3	Reverse TNCx2
2620	FCC/IC	Cushcraft	SL24513P	Omni, Single Feed	Indoor	2.4, 5	3	SMA-F

Table 138: Certified 3rd Party Antennas for Use with AP2620, AP260-1, AP3620 and AP3620-1 Models (continued)

AP	Regulatory	Manufacturer	Part Number	Type	Usage	Frequency	Gain	Connector
2620	FCC/IC	Cushcraft	S24497P	60 Deg Sector, Single Feed	Indoor	2.4, 5	7	Reverse TNC
2620	FCC/IC	Hyperlink	HG2458CU	Omni, Single Feed	Indoor	2.4, 5	3	N-F
2620	FCC/IC	Maxrad	MDO24005PT	Omni, Dual Feed	Indoor	2.4	5.2	SMA, TNC, N
2620	ETSI	Huber and Suhner	SOA 2454/360/7/20/DF	Omni	Outdoor	2.4, 5	6 & 8	N-F
2620	ETSI	Huber and Suhner	SWA 2459/360/4/45/V	Omni	Outdoor	2.4, 5	4	N-F/SMA-F
2620	ETSI	Huber and Suhner	SPA 2456/75/9/0/DF	Plannar	Outdoor	2.4, 5	9	SMA-F/TNC-F/QN-F
2620	ETSI	Huber and Suhner	SOA 2400/360/4/0/DS	Omni	Outdoor	2.4, 5	3.5	N-F/TNC-F
2620	ETSI	Huber and Suhner	SWA 0859/360/4/10/V	Omni	Outdoor	2.4, 5	7	N-F/TNC-F
2620	ETSI	Huber and Suhner	SPA 2400/80/9/0/DS	Plannar	Outdoor	2.4	8.5	SMA-F/TNC-F/QMA-F
2620	ETSI	Huber and Suhner	SPA 2400/40/14/0/DS	Plannar	Outdoor	2.4	13.5	N-F/TNC-F
3620	FCC/IC	Cushcraft	SR249120D	120 Deg, Sector, Single Feed	Indoor	2.4, 5	5	RPSMA
3620	FCC/IC	Cushcraft	S24493TS	Omni, Triple Feed	Indoor	2.4, 5	3	RPSMA 3 ea.
3620	FCC/IC	Cushcraft	SL24513WP	Omni	Indoor	2.4, 5	3	RPSMA
3620	FCC/IC	Cushcraft	S24497P	60 Deg Sector, Single Feed	Indoor	2.4, 5	7 & 8	RPSMA
3620	FCC/IC	Hyperlink	HG2458CU	Omni	Indoor	2.4, 5	3	N-F
3620	FCC/IC	Maxrad	MDO24005PT	Omni, Dual Feed	Indoor	2.4	5.2	RPSMA
3620	ETSI	Huber and Suhner	SOA 2454/360/7/20/DF	Omni	Outdoor	2.4, 5	6 & 8	N-F
3620	ETSI	Huber and Suhner	SWA 2459/360/4/45/V	Omni	Outdoor	2.4, 5	4	N-F/SMA-F
3620	ETSI	Huber and Suhner	SPA 2456/75/9/0/DF	Plannar	Outdoor	2.4, 5	9	SMA-F/TNC-F/QN-F

Table 138: Certified 3rd Party Antennas for Use with AP2620, AP260-1, AP3620 and AP3620-1 Models (continued)

AP	Regulatory	Manufacturer	Part Number	Type	Usage	Frequency	Gain	Connector
3620	ETSI	Huber and Suhner	SOA 2400/360/4/0/DS	Omni	Outdoor	2.4, 5	3.5	N-F/TNC-F
3620	ETSI	Huber and Suhner	SWA 0859/360/4/10/V	Omni	Outdoor	2.4, 5	7	N-F/TNC-F
3620	ETSI	Huber and Suhner	SPA 2400/80/9/0/DS	Plannar	Outdoor	2.4	8.5	SMA-F/ TNC-F/ QMA-F
3620	ETSI	Huber and Suhner	SPA 2400/40/14/0/DS	Plannar	Outdoor	2.4	13.5	N-F/TNC-F

C Default GuestPortal Ticket Page

Ticket Page

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 139: 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 139: 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 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>

```