Extreme Networks Extreme Management Center®

Wireless Manager User Guide

Legal Notices

Trademarks

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.,
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800

Toll-free: +1 888-257-3000

Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. <u>DEFINITIONS</u>. "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" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the 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 imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.

2. <u>TERM</u>. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications

and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. <u>GRANT OF SOFTWARE LICENSE</u>. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software 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. <u>LICENSE TYPES</u>.

- *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).

- *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 Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.

5. <u>AUDIT RIGHTS</u>. 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, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to

Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. <u>RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS</u>. 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 Software, or to translate the Licensed Software into another computer language.

   The media embodying the Licensed Software 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's 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. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. 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. <u>TITLE AND PROPRIETARY RIGHTS</u>

   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. <u>PROTECTION AND SECURITY</u>. 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's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) 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's 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 Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme

of any unauthorized use thereof. 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. <u>MAINTENANCE AND UPDATES</u>. 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 Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

10. <u>DEFAULT AND TERMINATION</u>. 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. <u>EXPORT REQUIREMENTS</u>. You are advised that the 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 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. <u>UNITED STATES GOVERNMENT RESTRICTED RIGHTS</u>. 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. <u>LIMITED WARRANTY AND LIMITATION OF LIABILITY</u>. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.
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. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. 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. <u>JURISDICTION</u>. 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. <u>GENERAL</u>.

   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's 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. 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: General Counsel

Table of Contents

Extreme Management Center Wireless Manager Overview (Legacy)

Wireless Manager simplifies network configuration by enabling you to configure and manage multiple Wireless Controllers and their associated wireless APs. Using Wireless Manager wizards and configuration tools, you can create a new network configuration or clone an existing one and apply that same configuration to multiple Wireless Controllers and APs.

Wireless Manager compares the configuration in its deployed templates to the actual configuration of managed Wireless Controllers. Wireless Manager logs an event and alerts you to any conflicts. Using the Conflict Resolution wizard, you can easily identify and address any discrepancies between the deployed templates and the actual configuration.

For general information about Wireless Manager, see the following sections:

- [Prerequisites](#)
- [Getting Started with Wireless Manager](#)
- [Understanding the User Interface](#)

Document Version

The following table displays the revision history for the Wireless Manager Help documentation.

Date	Revision Number	Description
04-17	8.0 Revision -00	Extreme Management Center 8.0 release
04-16	7.0 Revision -00	Extreme Management Center 7.0 release
07-15	6.3 Revision -00	NetSight 6.3 release
03-15	6.2 Revision -00	NetSight 6.2 release
06-14	6.1 Revision -00	NetSight 6.1 release

Date	Revision Number	Description
02-14	6.0 Revision -00	NetSight 6.0 release

PN: 9035084

Extreme Management Center Legacy Template Migration Notice (Legacy)

Wireless Manager no longer supports the configuration of Roles and Classes of Service (CoS). NetSight Policy Manager should be used for configuring Roles and CoS. Each time Wireless Manager is opened, if there are any legacy templates (Role, CoS, or Rate Profiles) defined, the following Legacy Template Migration notice appears:

The Legacy Template Migration notice indicates the number of days remaining before Wireless Manager terminates support for configuring Roles and CoS. For more information on configuring Roles, see Using Policy Manager to Create a Role Template. For more information on configuring CoS, see Using Policy Manager to Create a CoS Template.

Migrating Legacy Role and CoS Templates

If you have any legacy Role and CoS templates, they must be migrated within 30 days otherwise support will be terminated.

To migrate existing Role and CoS Templates:

1. Deploy your templates to the managed wireless controllers.

2. Using Policy Manager, assign your wireless controllers to a Policy domain and import their configuration. Select File > Import > Policy Configuration from Device.

3. From the Import from Device wizard, you must specify whether to import roles, rules, and/or class of services.

4. Save your changes.

5. Modify your Wireless Manager templates as needed to reference the newly created Role and CoS templates automatically imported from Policy Manager.

6. Remove the legacy templates. You can either delete the templates one-by-one or for your convenience use the following buttons displayed in the Legacy Template Migration dialog:

   - Brute-Force Cleanup – Deletes all legacy templates whether or not they are referenced by other templates. VNS templates may become "Incomplete". If Brute-Force Cleanup results in a VNS becoming "Incomplete", it will be displayed in the Conflict Resolution Wizard as a reminder for you to complete its definition and to specify a Non-Authenticated role for it.

   - Best-Effort Cleanup – Deletes all legacy templates not referenced by other templates.

   Please note these cleanup operations will even remove the legacy predefined CoS: Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, RTP/Voice/Video, and High Priority. However, upon synchronization with Policy Manager they will be automatically re-created, and will be consistent with their Policy Manager counterparts.

Extreme Management Center Wireless Manager Prerequisites

Before launching the Wireless Manager application, you should perform the following tasks:

1. Install or upgrade the NetSight server software.

2. Install your NetSight license. (If you are not using the NMS-BASE, NMS, or NMS-ADV licensing model, you will also need to install your Wireless Manager AP capacity licenses.) For licensing information, contact your Extreme Networks sales representative.

3. Launch NetSight Console.

4. In NetSight Console, create a full administrator account to be used by Wireless Manager to manage discovered Wireless Controllers.

5. Using the administrator credentials, create NetSight discovery profiles.

   Ensure that Wireless Controllers are discovered using an SNMP v2c or SNMP v3 profile. This profile must also contain SSH CLI credentials for the Wireless Controller. Wireless Manager uses the Wireless Controller's CLI to retrieve required device configuration data and to configure the managed Wireless Controllers.

   To configure the CLI credentials:

   a. From NetSight Console, access Tools > Authorization/Device Access > Profiles/Credentials tab.

   b. Select the CLI Credentials subtab.

   c. Select the CLI Credential being used by the Wireless Controller's Profile, and Click **Edit**.

   d. Enter the user name and password to be used in the credential. For Wireless Controllers, you must add the Login password to the Configuration field instead of the Login password field. The username and Configuration password specified here must match the username and Login password configured on the Wireless Controller.

   e. Verify the SSH connection type is selected.

f. Click **OK**.

g. Use this CLI Credential in the Wireless Controller's profile.

6. Discover Wireless Controllers using NetSight Console. Any Wireless Controllers that you discover will be available for viewing and configuration in Wireless Manager.

7. Optionally, from Wireless Manager, you can change the Langley protocol shared secret that is used for mutual authentication between a Wireless Controller and Wireless Manager.

Getting Started with Extreme Management Center Wireless Manager (Legacy)

When you first launch Wireless Manager, the following settings are in effect:

- Any Wireless Controllers that you previously discovered in NetSight are available for viewing and configuration.

- Any Mobility Zones created on the Wireless Controllers are listed in Wireless Manager.

- Any APs associated with the discovered Wireless Controllers are available for viewing and configuration. For each discovered Wireless Controller, Wireless Manager automatically creates a default AP group that includes all APs approved and active as local APs on that Wireless Controller.

To view discovered network elements:

1. Click Configured Objects > Wireless Networks and explore the discovered Wireless Controllers, Mobility Zones, and APs.
2. Click Configured Objects > AP Groups to explore the default AP groups created.

Configuring Controller Shared Secrets

Although you can immediately begin to configure your network after discovering the Wireless Controllers, you should change the shared secret on each Wireless Controller to provide additional security measures.

Wireless Manager uses a secure protocol called Langley to collect events and some configuration data from managed Wireless Controllers. The protocol is transported through an SSL/TLS tunnel. Shared secrets are used to mutually authenticate the two tunnel end points. Wireless Manager and Wireless Controllers ship from the factory with a common well-known shared secret. Having a default shared secret facilitates initial deployments but, unless you change the shared secrets, it can also provide a security risk because the shared secret is well known. Consequently, after Wireless Manager discovers a Wireless Controller, it is a best practice to change the shared secret used by Wireless

Manager and the Wireless Controller. You can configure Wireless Manager with a unique shared secret for each Wireless Controller managed by NetSight.

You cannot change the shared secret for a Wireless Controller until the Wireless Controller has been discovered. If you change the shared secret you must do so both on the Wireless Controller and on Wireless Manager.

To change the shared secret for a Wireless Controller, click Configured Objects > Wireless Networks > Generate Shared Secret and then assign/set the generated secret to the Wireless Controller.

Related Information

- [Extreme Management Center Wireless Manager Prerequisites](#)
- [Understanding the Wireless Manager User Interface (Legacy)](#)

Understanding the Wireless Manager User Interface (Legacy)

The Wireless Manager user interface provides a way to configure and manage Wireless Controllers and their associated APs. You navigate through the user interface as you would a typical web page, using the following components:

- [Global Menu Bar](#)
- [Global Button Bar](#)
- [Breadcrumb Trail](#)
- [Main Navigation Tabs](#)
- [Navigation Tree](#)
- [Context-Sensitive Toolbar](#)
- [Content Pane](#)
- [Event Tabs](#)

The following graphic shows the Wireless Manager main user interface page. See below for descriptions of each of the main components.
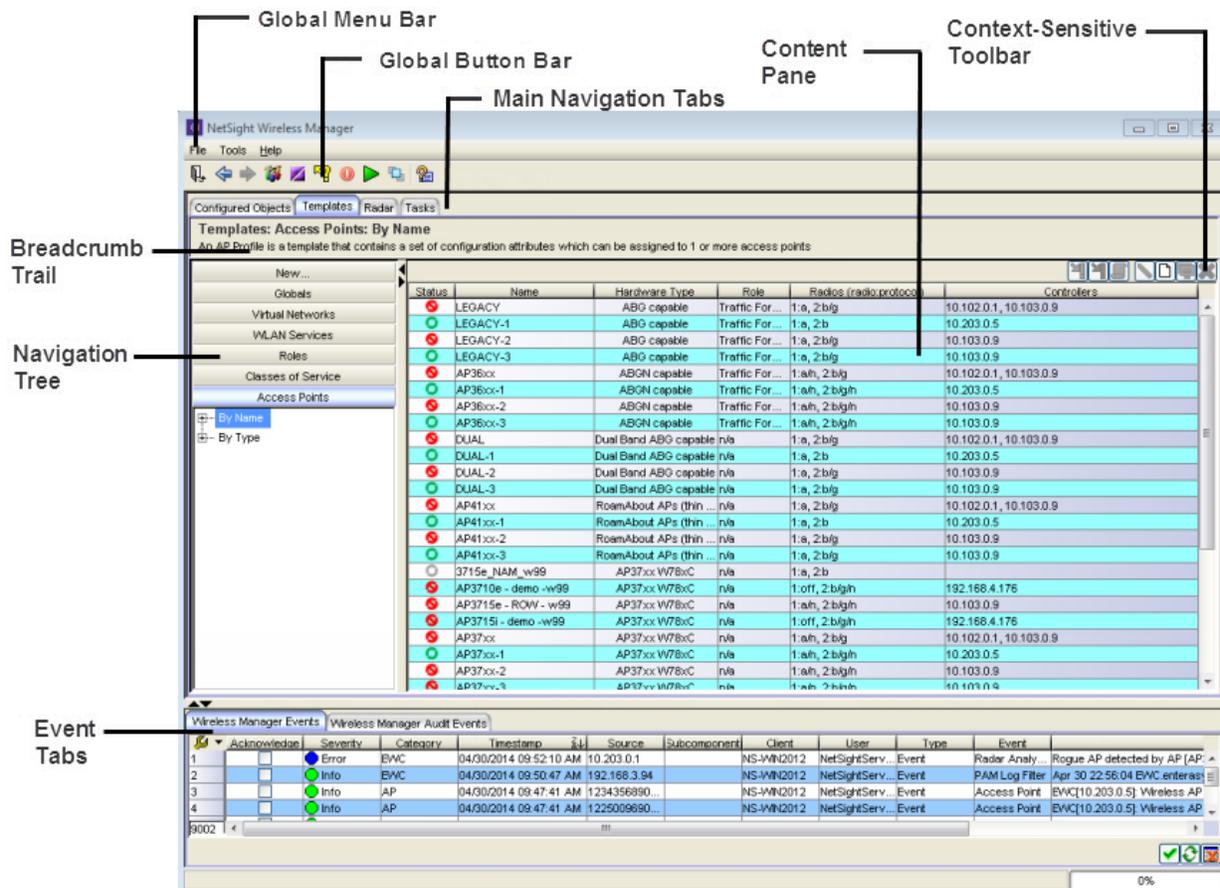
Global Menu Bar

The global menu bar displays across each page within Wireless Manager. Using the global menu bar, you can launch online help, access other Management Center tools, and perform Management Center management functions.

Global Button Bar

The global button bar is displayed across the top of each page.

The following list describes the function for each button.

Click to exit Wireless Manager.

Click to move backwards within Wireless Manager.

Click to move forward within Wireless Manager.

Click to configure user access to Extreme Management Center.

Click to view information about the Management Center server running the Wireless Manager application.

Click to run a configuration audit. If the audit detects any conflicts, you can launch the Resolve Audit Conflicts wizard to resolve them.

Click to launch the Resolve Audit Conflicts wizard. Use this wizard to resolve any conflicts between Wireless Manager's deployed templates and the actual Wireless Controller and AP configuration.

Click to poll and import data from all managed Wireless Controllers including: VNS, Topologies, WLANs, RADIUS Servers, Load Groups, Default AP Profiles, Global Settings, Radar Maintenance Settings and Scan Profiles.

Click to launch the Duplicate Resolution Wizard to detect and remove duplicate templates.

Click to view the online help for the page displayed in the right content pane.

Breadcrumb Trail

Use the breadcrumb trail to identify the path to the current page displayed in the user interface. The breadcrumb trail also displays an icon that shows the status of a configured network element.

Main Navigation Tabs

Below the buttons at the top of the page, there are four main navigation tabs that provide access to configuration information and settings for configured objects, templates, and tasks.

Following is a description of the functions of each navigation tab.

Configured Objects
Enables you to view and configure RADIUS and NAC servers, Wireless Controllers, network topologies, AP Groups and AP Load Groups. In addition, you can view information about Mobility Zones and wireless services.

Templates
Enables you to view, create and manage configuration in the form of templates for Globals, VNSs, WLAN Services, Roles, CoS, and AP Points.

Radar
Enables you to view, create, and manage in-service and Guardian scan profiles for detecting rogue devices and to provide countermeasures for resolving scan related issues. Enables you to manage Radar Maintenance templates for configuring how the Security Analysis Engine (on the controller) categorizes APs discovered in scan results.

Tasks
Enables you to view, create and manage tasks that update the configuration of managed Wireless Controllers and their APs.

Navigation Tree

The navigation tree displays in the left pane of the interface and is context-sensitive to the main navigation pane in use. You use the navigation tree to move among section bars and pages within the main navigation tab.

When a plus sign (+) displays next to an item in the navigation tree, you can click on it to show the hidden entries underneath. Conversely, you must click the minus sign (-) to collapse the display. The top-level folders collapse only when you expand a different top-level folder. When you click on an active link, the content of right-hand page refreshes. You can expand and collapse items in the

navigation tree without affecting the page content area displayed in the right pane; the right pane display changes only when you click another active link in the navigation tree.

Context-Sensitive Toolbar

The context-sensitive toolbar displays above the content page. The buttons that display are context-sensitive to the content page that displays. Buttons are disabled or grayed out when they are not active.

Deploy

Click to create a task to deploy this configuration.

Undeploy

Click to create a task to undeploy this configuration.

CLI Export

Click to export this configuration to a CLI script. For instructions, see Exporting a Configuration to the CLI in Extreme Management Center (Legacy).

Save

Click to save the configuration settings.

New

Click to create a new configuration.

Clone

Click to create a new configuration, using an existing configuration as a template.

Connect

Click to launch the Wireless Controller's Wireless Assistant GUI to view and configure the Wireless Controller. For more information, see Adaptive Management UI.

OneView

Click to connect to Management Center to view reports and statistics.

Reschedule

Click to open a Task wizard to select the date and time at which the Task will be deployed. Selections include Execute Immediately, Do not execute, and

Specify Time.

Execution Log

Click to open a save dialog to select a location for the selected task type file.

Retrieve

Click to import all entities (VNS, Topologies, WLANs, RADIUS Servers, Load Groups, Default AP Profiles, Radar Maintenance Settings, Scan Profiles) from all managed Wireless Controllers.

Edit

Click to change the configuration settings.

Delete

Click to delete the configuration.

Content Pane

The content section of each page displays information about the configured objects, templates and tasks as a form or table. You click a link in the page, or enter information in a field, to perform a task or to move among pages. You can also move among pages by clicking an object in the navigation tree.

Event Tabs

The Wireless Manager Audit and Wireless Manager Event tabs display across the bottom of the user interface. These tabs are not context-sensitive. Use the tabs as follows:

- Wireless Manager Audit tab — enables you to view the configuration activity on Wireless Manager.

- Wireless Manager Event tab — enables you to monitor and troubleshoot events.

Related Information

- Extreme Management Center Wireless Manager Prerequisites

- Getting Started with Extreme Management Center Wireless Manager (Legacy)

Exporting a Configuration to the CLI in Extreme Management Center (Legacy)

You can export a configuration to the Wireless Controller's CLI by launching the Export wizard.

1. To launch the Export wizard, click on the object and click the CLI Export button .

2. **Select Placeholder Option.** Select whether to export this configuration to a specific Wireless Controller or to use a placeholder for the Wireless Controller. Click **Next**.

3. **Choose a Filename.** Navigate through your system and identify a name for the export file and the directory in which to store this file. By default, the system appends the .cli extension to the filename. Click **Finish**.

4. **Saving File to Disk.** A message displays stating whether the file export was successful.

5. Click **Close** to close the window or click **View Log** to view detailed log information about the task.

Managing Configured Objects in Extreme Management Center (Legacy)

Configured objects are the building blocks of configuration templates. You must either discover or manually identify the network's configured objects before you can create or deploy templates to configure your wireless network using Wireless Manager.

This section includes the following topics:

- [About Network Servers](#) for information about NAC and RADIUS servers.
- [About Network Topologies in Extreme Management Center (Legacy)](#) for information about network topologies.
- [About Wireless Networks in Extreme Management Center (Legacy)](#) for information about shared secrets, controllers, and mobility zones.
- [About Wireless Services](#) for information about SSIDs.
- [About AP Groups](#) for information about creating and managing AP groups.
- [About AP Load Groups](#) for information about creating and managing AP Load Groups.

About Network Servers in Extreme Management Center (Legacy)

Network servers include NAC servers and RADIUS servers. This Help topic includes the following information:

- [About NAC Servers](#)
  - [Creating a NAC Server Configuration](#)
  - [Viewing Summary Information about Configured NAC Servers](#)
  - [Viewing Detailed Information about a Configured NAC Server](#)
  - [Modifying the NAC Server Configuration](#)
  - [Deleting the NAC Server Configuration](#)
- [About RADIUS Servers](#)
  - [Creating a RADIUS Server Definition](#)
  - [Viewing a RADIUS Server Configuration](#)
  - [Editing the RADIUS Server Configuration](#)
  - [Deleting a RADIUS Server Configuration](#)

About NAC Servers

A Network Access Control (NAC) server from Extreme Networks provides enhanced system-level controls to protect your network from unwanted or unauthorized access. The wireless infrastructure sees the NAC server as a RADIUS server with an external captive portal.

You can use the NAC server definition when you define a VNS or WLAN service that requires RADIUS servers. When you deploy the VNS configuration to a Wireless Controller, the NAC server's web interface is configured as an external captive portal and the NAC server's RADIUS interface is configured as the RADIUS server for authentication.

Using Wireless Manager, you can create a NAC server configuration that determines how Wireless Controllers will interact with a particular NAC server. You cannot, however, create the actual NAC server or create the configuration data that is sent to a NAC server.

Creating a NAC Server Configuration

When creating a NAC server configuration, you define how Wireless Controllers will interact with a particular NAC server. After you create a new NAC server configuration, you must create a task to deploy the configuration or the settings will not take effect.

In the NAC server configuration, you can configure the following:

Radius Related Settings

- Server Details
  - Name of the NAC server that is used by Wireless Manager to simplify server identification.
  - IP address and shared secret to use for RADIUS interactions.
  - Default Protocol: PAP, CHAP, MS-CHAP, MS-CHAP2.
- Authentication
  - Total Number of Tries, RADIUS Request Timeout, Port.
- Health Monitoring
  - Polling Mechanism, Test Request Timeout.

Captive Portal Settings

- NAC Details
  - IP address to use for captive portal redirection.

To create a new NAC server configuration:

1. Click the Configured Objects tab. The Configured Objects main page displays.

2. In left-hand pane, click New, expand the New icon, and click NAC server. The NAC Server Configuration page displays.

3. Enter the appropriate information in the fields on the page. For a definition of each field, see below.

4. Click the **Save** button on the toolbar.

NOTE: To create a new NAC server definition from the NAC Server Summary page, you can either click on the New icon or right-click on a configured object in the summary window to display a pop-up menu, from which you can click on the New icon to display the NAC Server Configuration page.
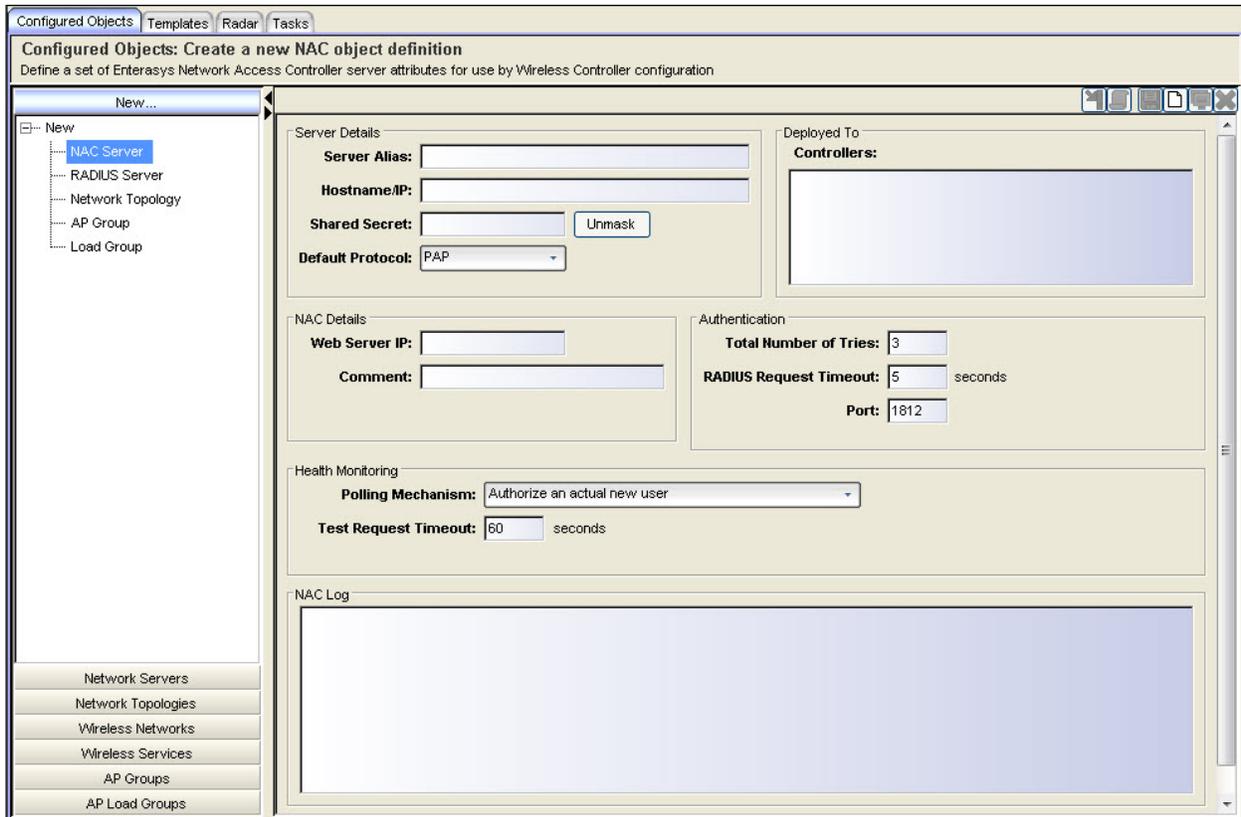
The following list describes the information available on the NAC Server Configuration page.

Server Details

Server Alias
> The name you assign to the NAC server.

Hostname/IP
> The IP address assigned to the server.

Shared Secret
> The password that will be used to validate the connection between the Wireless Controller and the NAC server.

Unmask/Mask
> Click this button to view/hide the shared secret.

Default Protocol
> Select the default authentication protocol. Options include: PAP, CHAP, MS-CHAP, MS-CHAP2.

NAC Details

Web Server IP
IP address assigned to the web server.

Comment
Descriptive information about the NAC server.

Deployed To
Controllers
Wireless Controllers to which this NAC server configuration is deployed.

Authentication
Total Number of Tries
Default is 3 retries.

RADIUS Request Timeout
Default is 5 seconds.

Port
Default is 1812.

Health Monitoring
Polling Mechanism

Select the Polling Mechanism from the drop-down to be used to detect if the primary server has recovered. Options include:

Authorize an actual new user (default):

Periodically the EWC will attempt to authenticate a user using the primary server.

- If the authentication succeeds all subsequent client authentications will use the primary server.
- If the client fails to authenticate, use the known working RADIUS server instead.
- Assumes clients are being periodically authenticated.

Use RFC 5997 Status-Server Request:

Periodically the EWC will send a Status-Server request to the primary server.

- If a response is received then all subsequent client authentications will use the primary server.

- If no response is received, then the known working RADIUS server will continue to be used.

- Assumes the RADIUS server supports RFC 5997.

Test Request Timeout

Enter a Test Request Time to specify how often to check if the primary server is up (range [30, 300], default is 60 seconds).

NAC Log

Tracks any changes made to the NAC server.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Viewing Summary Information about Configured NAC Servers

You can view summary information about NAC servers currently defined in Wireless Manager from the NAC Server Summary page. From this page, you can also perform the following tasks:

- Edit, clone, undeploy, or delete an existing NAC server definition.

- Export a NAC server configuration to the CLI.

- Create new NAC server definition.

To view information about configured NAC servers:

1. Click the Configured Objects tab

2. In left-hand pane, click Network Servers > NAC Servers. The NAC Server Summary page displays. For a definition of each field, see below.
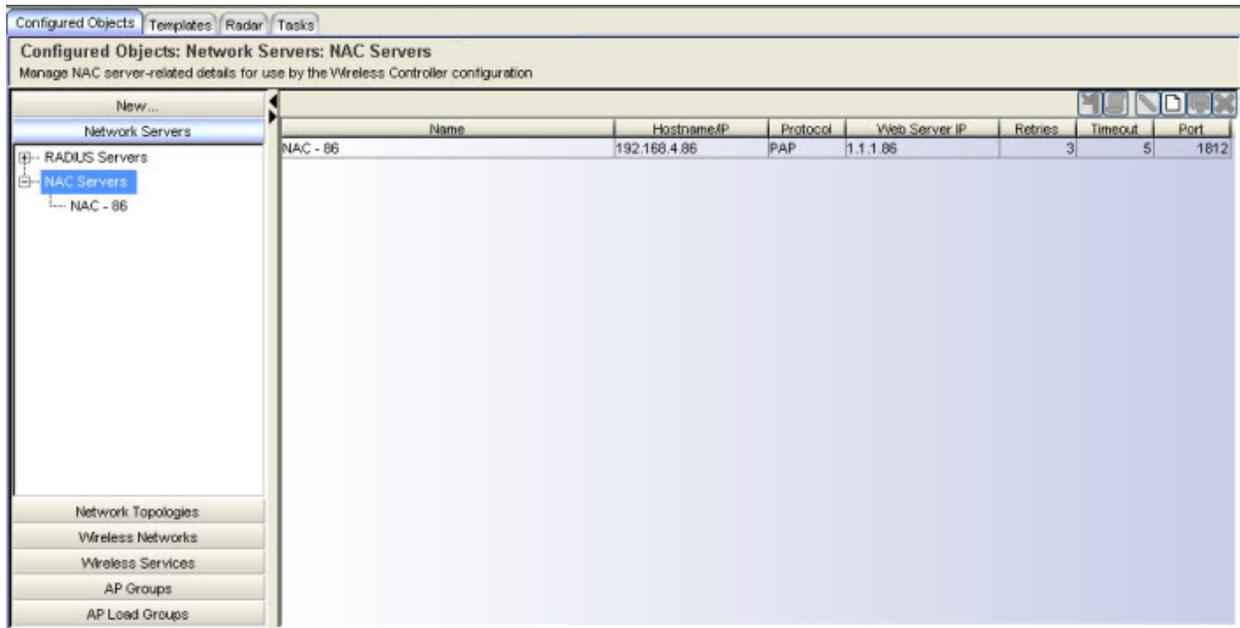
The following list describes the information available on the NAC Server Summary page.

Name

The name of the NAC server available on your network.

Hostname/IP

The IP address of the NAC server on your network.

Protocol

Data authentication protocol in use. Options include: PAP, CHAP, MS-CHAP, MS-CHAP2.

Web Server IP

The NAC web server IP address.

Retries

The number of times Wireless Manager tries to contact the NAC server before failing over to another NAC server.

Timeout

Default is 5 seconds.

Port

Default Authentication port is 1812.

Toolbar Buttons

For a description of common toolbar buttons see Context-Sensitive Toolbar.

Viewing Detailed Information about a Configured NAC Server

You can view detailed information about NAC servers currently defined in Wireless Manager from the NAC Server Details page. From this page, you can also perform the following tasks:

- Edit, clone, undeploy, or delete an existing NAC server definition.
- Export a NAC server configuration to the CLI.
- Create new NAC server definition.

To view information about configured NAC servers:

1. Click the Configured Objects tab.
2. In left-hand pane, click Network Servers > NAC Servers. The NAC Server Summary page displays.
3. In the left-hand pane, click on a NAC server name from the list. The NAC Server Details page for that task displays. For a definition of each field, see below.

The following list describes the information available on the NAC Server Details page.

Server Details

Server Alias

The name you assign to the NAC server.

Hostname/IP

The IP address assigned to the server.

Shared Secret

The password used to access the server.

Unmask/Mask

Click this button to view/hide the shared secret.

Default Protocol

PAP, CHAP, MS-CHAP, MS-CHAP2.

NAC Details

Web Server IP

IP address assigned to the web server.

Comment

Descriptive information about the NAC server.

Deployed To

Controllers

Wireless Controllers where the NAC server is deployed.

Authentication

Total Number of Tries

Default is 3 retries.

RADIUS Request Timeout

Default is 5 seconds.

Port

Default is 1812.

NAC Log

Tracks any changes made to the NAC server.

Toolbar Buttons

For a description of common toolbar buttons see Context-Sensitive Toolbar.

Modifying the NAC Server Configuration

You can change the NAC server configuration at any time. Changes will not take effect until you create a task to deploy the changed configuration.

To edit a NAC server configuration:

1. Click the Configured Objects tab.

2. Select a NAC server on the NAC Server Summary page and either click the edit icon at the top of the page or right-click on the task name and select Edit from the pop-up menu. The NAC Server Details page displays.

3. Change the configuration as needed and save the configuration changes by clicking the **Save** button. These changes will be deployed the next time a template referencing this NAC server is deployed.

Deleting the NAC Server Configuration

You can delete a NAC server configuration as long as it is not currently in use. You must remove it from all Wireless Controllers to which it has been deployed before you can delete it.

To delete a NAC server configuration:

1. Click the Configured Object tab.

2. Select a NAC server on the Server Summary page and either click the delete icon at the top of the page or right-click on the NAC server name and select Delete from the drop-down menu. A confirmation dialog box displays.

3. Click **OK** to delete the NAC server configuration. The NAC Server Details page displays with the updated information.

About RADIUS Servers

RADIUS servers provide authentication, authorization, and accounting functions in your network. Using NetSight Wireless Manager you can create RADIUS server definitions by retrieving them from discovered Wireless Controllers or by entering the configuration manually. After identifying and defining the RADIUS servers, you can create a task to deploy the RADIUS server definition to one or more Wireless Controllers.

NOTE: Using Wireless Manager, you cannot create the actual RADIUS server or create the configuration data that is sent to a RADIUS server.

Creating a RADIUS Server Definition

You can create a RADIUS server definition either manually or by polling the discovered Wireless Controllers.

When you manually create a RADIUS server definition, you must provide the following information:

- Name used by Wireless Manager to identify the RADIUS server
- IP address or hostname of the RADIUS server
- Shared secret
- Default protocol

When you poll Wireless Controllers for a list of RADIUS servers, Wireless Manager provides a list of all RADIUS servers known to the discovered Wireless Controllers. Wireless Manager merges the lists of RADIUS servers collected from different Wireless Controllers. If more than one Wireless Controller assigns different attributes to the same RADIUS server (identified by IP address), the merge list includes that RADIUS server multiple times and adds a suffix (-1, -2, and so on) to the server name to distinguish between them.

You can view and clean up any discrepancies, and then deploy the corrected lists back to the Wireless Controllers.

Polling the Controllers for RADIUS Servers

To poll the discovered Wireless Controllers for RADIUS servers:

1. Click the Configured Objects page.
2. Click Network Servers > RADIUS Servers. The RADIUS Server Summary page displays.
3. Click the **Poll Controllers** button. Wireless Manager queries each Wireless Controller that it manages for its list of RADIUS servers and populates the RADIUS Server Summary page (see Radius Server Summary Page) with the results.

Manually Creating a RADIUS Server Definition

To create a RADIUS server definition:

1. Click the Configured Objects tab.

2. Click Network Servers > RADIUS Servers. The RADIUS Server Configuration page displays. From the RADIUS Server Configuration page, you can create a new RADIUS server definition or change one that has already been created. For a definition of each field, see below.

NOTE: You can also access the RADIUS Server Configuration from the Configured Objects tab by clicking New > RADIUS server.
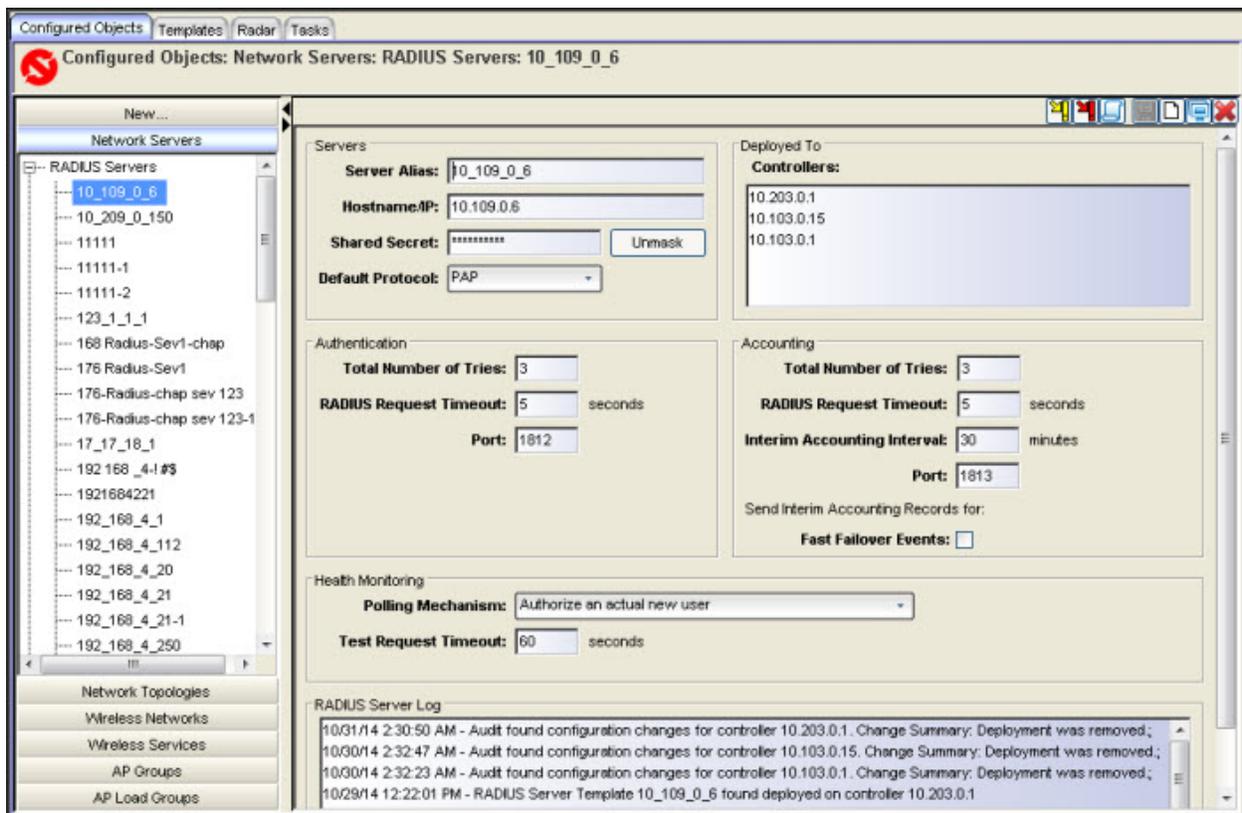
The following list describes the information available on the RADIUS Server Configuration page.

Servers
Server Alias
   The name Wireless Manager uses to identify the RADIUS server.

Hostname/IP
   The RADIUS server's FQDN (fully qualified domain name) or IP address.

Shared Secret
> The password used to validate the connection between the Wireless
> Controller and the RADIUS server.

Unmask/Mask
> Click Unmask to view your shared secret key. Click Mask so that the shared
> secret is not visible on the screen.

Default Protocol
> If desired, change the **Default Protocol** using the drop-down list. Choices are
> PAP, CHAP, MS-CHAP, or MS-CHAP2.

Authentication

Total Number of Tries
> Enter a value for the number of authentication tries. Default is 3 tries.

RADIUS Request Timeout
> Default is 5 seconds.

Port
> Default accounting port is 1813.

Deployed To

Controllers
> Lists all Wireless Controllers to which this RADIUS server definition has been
> deployed.

Accounting

Total Number of Tries
> Default is 3 tries.

RADIUS Request Timeout
> Default is 5 seconds.

Interim Accounting Interval
> Default is 30 minutes.

Port
> Default accounting port is 1813.

Fast Failover Events
> Click to allow the controller receiving the session to immediately begin
> sending out interim accounting records. This feature can be enabled for any
> type of authentication and applies only to controllers in availability with fast
> failover enabled. Default is disabled.

Health Monitoring

Polling Mechanism

Select the Polling Mechanism from the drop-down to be used to detect if the primary server has recovered. Options include:

Authorize an actual new user (default):

Periodically the EWC will attempt to authenticate a user using the primary server.

- If the authentication succeeds all subsequent client authentications will use the primary server.
- If the client fails to authenticate, use the known working RADIUS server instead.
- Assumes clients are being periodically authenticated.

Use RFC 5997 Status-Server Request:

Periodically the EWC will send a Status-Server request to the primary server.

- If a response is received then all subsequent client authentications will use the primary server.
- If no response is received, then the known working RADIUS server will continue to be used.
- Assumes the RADIUS server supports RFC 5997.

Test Request Timeout

Enter a Test Request Time to specify how often to check if the primary server is up (range [30, 300], default is 60 seconds).

RADIUS Server Log

Tracks any changes made to the RADIUS server.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Viewing a RADIUS Server Configuration

The RADIUS Server Summary page shows the RADIUS server information available for you to deploy to Wireless Controllers. From the RADIUS Server summary page, you can also perform the following tasks:

- Poll all managed Wireless Controllers to automatically create templates for existing RADIUS servers.

- Reprioritize the RADIUS servers according to accounting settings.

- Reprioritize the RADIUS servers according to authorization settings.

- Deploy or undeploy the server configuration.

- Edit or clone an existing server configuration.

- Export the configuration to the Wireless Controller's CLI.

- Create a new RADIUS server configuration.

To view the configuration for a RADIUS server:

1. Click the Configured Objects tab.

2. In left-hand pane, click Network Servers > RADIUS Servers. The RADIUS Server Summary page displays. For a definition of each field, see below. To configure the RADIUS server characteristics, see Creating a RADIUS Server Definition.

The following list describes the information available on the RADIUS Server Summary page.

Status

Status of this RADIUS server. The possible status values are:

   Not deployed - the RADIUS server definition has not been deployed to any Wireless Controllers.

⬤ Deployed in sync - the RADIUS server definition has been deployed to at least one Wireless Controller and all controllers to which this definition has been deployed have the same configuration as the one on Wireless Manager. 🚫 Deployed not in sync - the RADIUS server definition has been deployed to at least one Wireless Controller. At least one controller to which this definition has been deployed has a conflicting definition for this RADIUS server.

Server Alias

The name Wireless Manager uses to identify the RADIUS server.

Server Hostname/IP

The RADIUS server's FQDN (fully qualified domain name) or IP address.

Default Protocol

Default protocol is the default authentication mechanism used by this RADIUS server.

Retries - Auth

Number of times the Wireless Controller should try to send an authentication request to this server when no response is received.

Retries - Acct

Number of times the Wireless Controller should try to send an accounting request to this server when no response is received.

Timeout - Auth

Time to wait for a reply to an authentication request sent to this RADIUS server.

Timeout - Acct

Time to wait for a reply to an accounting request sent to this RADIUS server.

Ports - Auth

Port on the RADIUS server to which authentication requests should be sent.

Ports - Acct

Port on the RADIUS server to which RADIUS accounting records should be sent.

Priority - Auth

The default priority of the RADIUS server relative to other RADIUS servers on the EWC for purposes of authentication. The priority is used to select which RADIUS server the Wireless Controller's RADIUS client will send to first. The server with the lowest numbered priority will be used as the primary RADIUS server for authentication. A controller will use up to three RADIUS servers per

WLAN Service for authentication. The controller will use the second and third priority servers as fallback servers if necessary.

Priority - Acct

The priority of this RADIUS Server relative to other RADIUS servers for use as accounting servers by the EWC.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Editing the RADIUS Server Configuration

You can edit the attributes of the RADIUS servers. After you finish editing the configuration, Wireless Manager updates the status of the RADIUS Server definition to show that the change has not been deployed.

The status is updated after you deploy the configuration.

The list of RADIUS servers on the Wireless Manager has a priority ordering for accounting and a different priority ordering for authentication. These orderings act as defaults if you include the RADIUS server in a VNS definition. When you create a task to deploy a VNS or WLAN Service, you have the option of customizing, per Wireless Controller, which RADIUS servers are actually used and the order of preference of the selected servers for authentication and accounting.

Wireless Manager has a single list of all the RADIUS servers that it uses when creating a VNS. However it does not force each of the Wireless Controllers to maintain exactly the same list. You can enable different controllers to use different subsets of the list.

To edit the configuration for a RADIUS server:

1. Click the Configured Objects tab.

2. In left-hand pane, click Network Servers > RADIUS Servers. The RADIUS Server Summary page displays.

3. Select a RADIUS server on the RADIUS Server Summary page and either click the edit icon at the top of the page or right-click on the RADIUS server name and select Edit from the drop-down menu. The RADIUS Server Configuration page displays.

4. Configure individual settings as needed. For more information, see [Creating a RADIUS Server Definition](#).

5. Click **Save**.

Deleting a RADIUS Server Configuration

You cannot delete a RADIUS server definition until it is no longer assigned to any WLAN Service.

To delete a RADIUS server configuration:

1. Click the Configured Objects tab.

2. In left-hand pane, click Network Servers > RADIUS Servers. The RADIUS Server Summary page displays.

3. Select a RADIUS server definition on the RADIUS Server Summary and either click the delete icon at the top of the page or right-click on the task name and select Delete from the drop-down menu.

4. The Delete RADIUS Server wizard appears with various options.

5. Click **OK** to delete the RADIUS server definition.

6. The RADIUS Server Summary displays with the updated information.

About Network Topologies in Extreme Management Center (Legacy)

A topology, which is a combination of Layer 2 and possibly Layer 3 networking attributes, represents the networks with which the Wireless Controller and its APs interact. The main configurable attributes of a topology are:

- Type — How traffic is forwarded on the topology. Options are:
  - Routed — the Wireless 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 Wireless Controller.
- Interface — The IP (L3) address assigned to the Wireless Controller on the network described by the topology (Optional).
- VLAN ID and associated L2 port.
- 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.

You can define a topology on a Wireless Controller that is not attached to any service. You can also create a VNS definition that includes a Role or WLAN that uses the topology, and apply it to a Wireless Controller when required.

Although most topology settings can apply to all Wireless Controllers, you must customize some topology settings for each Wireless Controller. For example, Wireless Manager lets you assign the same topology to different ports on different Wireless Controllers during template deployment. You can customize topology settings per Wireless Controller when you deploy the topology to a Wireless Controller either directly or as part of deploying a VNS, WLAN, or Role.

This Help topic includes the following information:

Creating a Network Topology Configuration

You can create a network topology definition either manually or automatically by:

- retrieving topology configurations directly from managed Wireless Controllers, or
- assigning devices to Policy Manager domains which include roles that restrict the Wireless Default Access Control to a particular VLAN, that include egress VLANs, or that have rules that Contain to VLAN.

If you poll the Wireless Controllers for topology definitions, Wireless Manager merges the topologies into a single coherent list. If the same topology (identified by name) exists on more than one Wireless Controller with conflicting settings, then Wireless Manager records the topologies as two separate topologies and for each topology name appends the suffix (-1, -2, and so on) to distinguish them.

If you are using Policy Manager, after you save the configuration for a particular domain which includes Wireless Controllers, Wireless Manager will automatically create for you those topologies corresponding to the global VLANs in the domain. This includes those topologies referenced by roles which restrict Wireless Default Access Control to a particular VLAN, that include egress VLANs, or that have rules that Contain to VLAN.

Topologies created on behalf of Policy Manager:

- Can be easily identified in the Topology Tree since their names include the name of the Policy Manager domain from which they were created.
- Cannot have their VLAN IDs or names changed.

- Only support mode changes between Bridged at Controller, Bridged at AP, and Routed.
- Cannot be deleted so long as Policy Manager has a VLAN defined which references it.

For details about how to create roles in Policy Manager, please refer to the NetSight Policy Manager User Guide.

A topology definition includes the following:

- General Settings
- Multicast Filters - Defines the multicast groups that are allowed on a specific topology segment.
- Exception Filters - Specifies which traffic has access to the Wireless Controller from the wireless clients or the infrastructure network.
- Per Controller L2/L3 Settings

General Settings

A topology's general settings determine basic functionality, including the following:

- Name of the topology.
- Mode used for forwarding data traffic.
- Compatibility used to identify deployable Wireless Controller software versions for the topology template.
- L2 and/or L3 Settings.
- Topology Log for tracking any changes made to the topology.

Manually Creating a Network Topology Configuration

To manually create a network topology configuration:

1. Click the Configured Objects tab.
2. In left-hand pane, click New, expand the New icon and select Network Topology. The Network Topology Configuration page displays with the General tab selected.
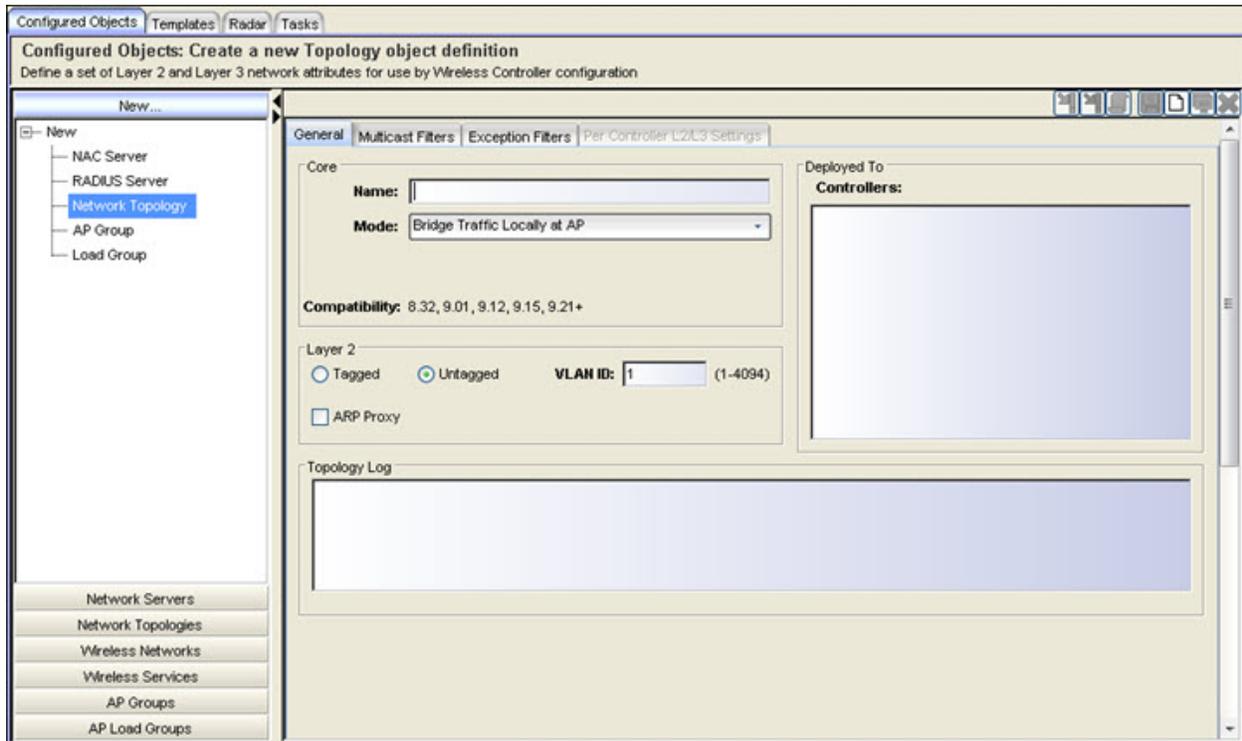
The following list describes the information available on the Network Topologies General tab.

Core

Name

Name assigned to identify the network topology.

Mode

Describes how traffic is forwarded on the topology. Options include:

Routed – Does not need any Layer 2 configuration, but does require Layer 3 configuration.

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 HWC – Requires Layer 2 configuration. May optionally have Layer 3 configuration. Layer 3 configuration is necessary if services (such as DHCP, captive portal, and so on) are required over the

configured network segment, or if Wireless Controller management operations are intended to be done through the configured interface.

Topology Group

Select to add a topology group attribute to the network topology. Topology groups load balance stations over a set of VLANs.

Selecting Topology Group displays the Topologies section.
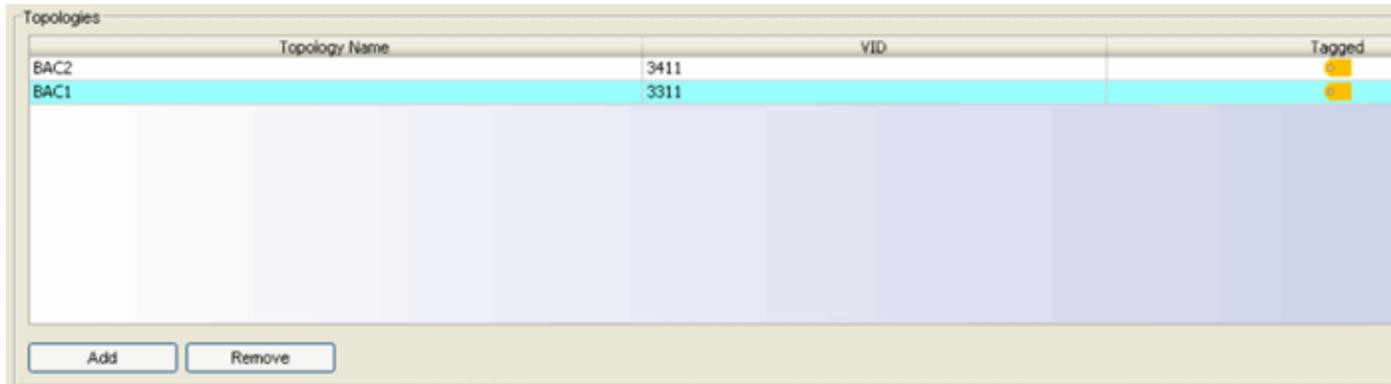
The Topologies section allows you to add topology templates of the same Type to a topology group.

NOTES: **Topology Group** is only available for network topologies with a **Mode** of **Routed** or **Bridge Traffic Locally at Controller**.

Topology Group is NOT available on:

- Wireless Controllers with versions earlier than 9.21.
- APs with versions of 2600 or 3600.
- B@AP topologies.
- Sites.
- Another Topology Group.

Compatibility

Identifies deployable Wireless Controller software versions for the topology template.

Layer 2

Tagged

Select to specify VLAN tagging.

Untagged

Select to disable VLAN tagging.

VLAN ID

The unique VLAN identifier as specified in the IEEE 802.1Q definition. The **VLAN ID** can be referenced from PM created roles (e.g. default VLAN, egress VLANs) and rules. If a Wireless Manager Routed or B@AP (untagged) Topology doesn't have a valid **VLAN ID** on deployment, the **VLAN ID** dialog displays. You can select from one of the recommended **VLAN ID**s or enter a new ID not currently in use by another topology or topology group. **VLAN ID**s can be any value between 1 and 4,094.

ARP Proxy

Select to have the AP serve as ARP Proxy for those clients associated to the AP for this particular topology. Selecting ARP Proxy, allows the AP to reply to ARP requests rather than broadcasting them over the air.

Layer 3

Layer 3 Presence

Select to apply DHCP and IP options when the Network Topology is deployed.

MTU

Maximum transmission unit.

Management Traffic

Select to enable management traffic for a topology.

Deployed To

Controllers

One or more Wireless Controllers that have been configured to use this network topology.

Topology Log

Tracks any changes made to the topology.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Multicast Filters

You can enable multicast traffic as part of a topology definition 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 Multicast Forwarding checkbox.

From the Multicast Filters tab, you can define a list of multicast groups whose traffic is allowed to be forwarded to and from a VNS using this topology. The default behavior is to drop the packets. For each group defined, you can enable Wireless Replication by group. Wireless Replication applies to multicast traffic coming from the wireless network and whether or not to replicate it back to the wireless network. Multicast traffic received from the wireless network is always transmitted to the wire.

NOTE: After enabling multicast filters for a routed topology, you will need to define which physical topology to use for global multicast support. This is done at deployment time when you specify the per-Wireless Controller deployment settings for the topology.

Configuring multicast filters for a Topology

To view the multicast filter fields:

1. Click the Multicast Filters tab. The Network Topology Configuration Page Multicast Filters tab displays.
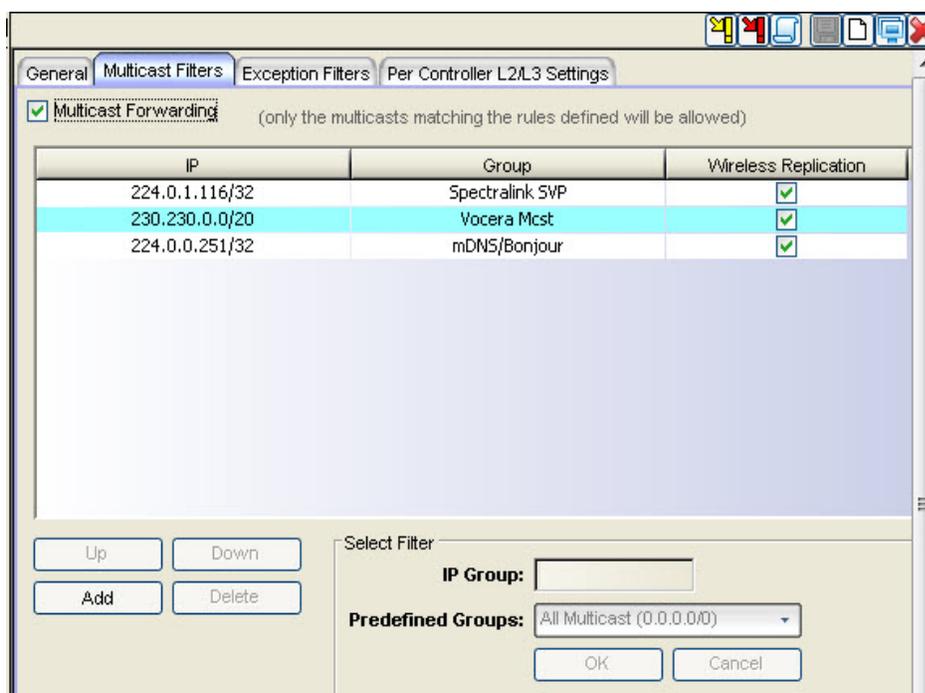
The following list describes the information available on the Multicast Filters tab.

Multicast Forwarding
Select to enable the multicast function.

IP
IP Address.

Group

Multicast group.

Wireless Replication

To enable the wireless multicast replication for this group, select the **Wireless Replication** checkbox.

Up | Down | Add | Delete

Select a filter from the Predefined Groups drop-down menu:

Click Add to add a predefined filter.

Click Delete to remove a predefined filter.

Click Up to raise the priority of the selected multicast group.

Click Down to lower the priority of the selected multicast group.

Select Filter

IP Group

The IP range for multicast groups.

Predefined Groups

Select from the list of predefined multicast group (includes User Defined).

OK

Click to save the configuration.

Cancel

Click to discard the changes to the configuration.

To configure multicast filters for a topology:

1. Select **Multicast Forwarding** to enable the multicast function.

2. Define the multicast groups by using the following controls:

    - **IP Group** – Type the IP address range.

    - **Predefined groups** – Click from the drop-down list

3. Click **Add**. The group is added to the list above.

4. To enable the wireless multicast replication for this group, select the corresponding **Wireless Replication** checkbox.

5. To modify the priority of the multicast groups, click the group row, and then click the **Up** or **Down** buttons. Only the multicast traffic matching the rules defined on the page will be allowed.

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

Exception Filters

CAUTION: 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.

For bridged at Wireless Controller topologies, you can define exception filters only if L3 (IP) interfaces are specified. For routed topologies, exception filtering is always configured since they all have an L3 interface presence.

On the Wireless Controller, various interface-based exception filters are built in and invoked automatically. These filters protect the Wireless 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 when the topology configuration has **allow management** traffic enabled. Users will only be able to target the topology interface specifically.

On the L3 interfaces (associated with either routed, or bridged locally at Wireless 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 Wireless 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 filtering rules, in the case of traffic from wireless users, are applicable to traffic targeted directly for the topology L3 interface. Exception filter rules are evaluated after the user's assigned filter policy, as such, it is possible that the policy 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. Navigate to the details page of a specific Bridged at EWC or routed topology.

2. Click the Exception Filters tab. If your topology type is Bridged at EWC, you will have to first select the Layer 3 Presence checkbox. The Exception Filters tab is displayed.

3. Select the **Management Traffic** checkbox if the topology has specified an L3 IP interface presence.

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

You can add specific filtering 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 filtering rules are set up in the same manner as filtering rules defined for a Policy — specify an IP address, select a protocol if applicable, and then either allow or deny traffic to that address.

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).

To define interface exception filters:

1. Click the Configured Objects tab.

2. In the left pane, click Network Topologies. The Network Topologies screen is displayed.

3. Select a topology to be configured. The Edit Topology window is displayed.

4. Select the Exception Filters tab. The Exception Filter page displays.

NOTE: The Exception Filters tab is available only if you defined an L3 interface for the topology
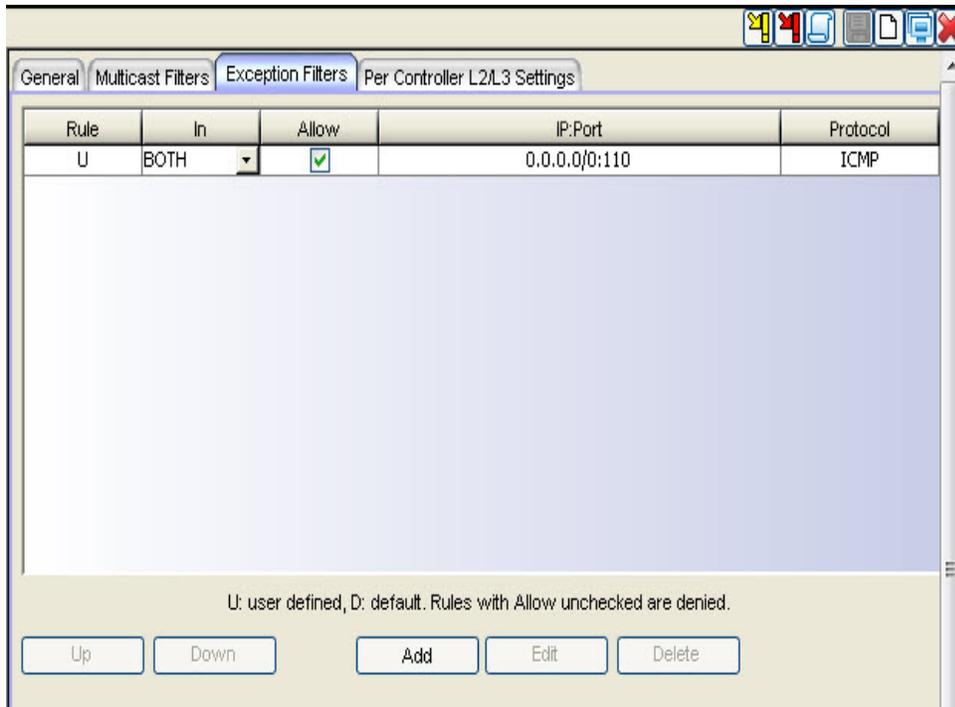
The following list describes the information available on the Exception Filters tab.

Rule

Identifies the type of filter rule. Options Include: D - Default rule, and U - user-defined rule.

In

Identifies how to filter traffic coming into the network from the wireless stations. Check the rule's checkbox in this column to have the rule applied. The list includes: **Destination** (dest), **Source** (src), **None**, and **Both**.

Allow

Check the rule's checkbox in this column to cause traffic matching this rule to be forwarded. Clear the checkbox in this column to have the rule deny traffic that matches the rule.

IP: Port

IP address, or address and optionally port or port range to which this rule applies.

Protocol

The particular protocol to which this rule applies.

Up | Down | Add | Delete

Click Add to specify the details of the filter rule to be added.

Click Delete to remove the selected filter rule.

Click Up to raise the priority of the selected filter rule.

Click Down to lower the priority of the selected filter rule.

IP/Subnet
The IP address to filter on. You can also specify an IP range, a port designation, or a port range on that IP address.

Port
Specifies a port designation, or a port range on the IP address.

Protocol
Click the protocol you want to specify for the filter. This list may include **UDP**, **TCP**, **GRE**, **IPsec-ESP**, **IPsec-AH**, **User Defined**, and **ICMP**. The default is N/A.

In Filter
Click an option that refers to how to filter traffic coming into the network from wireless stations. This list includes: **Destination** (dest), **Source** (src), **None**, and **Both**. The default is None.

OK
Click to save changes.

Cancel
Click to discard changes.

To configure exception filters:

1. Click the **Add** button. The Filter Editor dialog appears in a separate window.

2. Fill in the following fields:

   In the **IP/subnet** box, type the destination IP address. Using the Port drop down, you can also specify a User Defined or well-known port to filter on for the specified IP. 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**, **User Defined**, and **N/A**. The default is N/A.

   In the In Filter field, select a mode for filtering traffic going inbound from

the Mobile Unit (MU) into the network. Options include **Destination**, **Source**, **None**, and **Both**.

3. The new filter displays Exception Filters page.

4. Click the new filter entry.

5. To allow traffic, select the **Allow** checkbox.

6. To adjust the order of the filtering rules, click **Up** or **Down** to position the rule. The filtering rules are executed in the order defined here.

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

Per Controller L2/L3 Settings

Per Controller settings are read-only in the template. To change them, you must create a task to redeploy the template with the new settings.

To view the Per Controller L2/L3 Settings:

1. Click the Configured Objects tab.

2. In the left pane, click Network Topologies. The Network Topologies page displays.

3. Select a topology. The Edit Topology page displays.

4. Select the Per Controller L2/L3 Settings tab. The Per Controller L2/L3 Settings page displays.
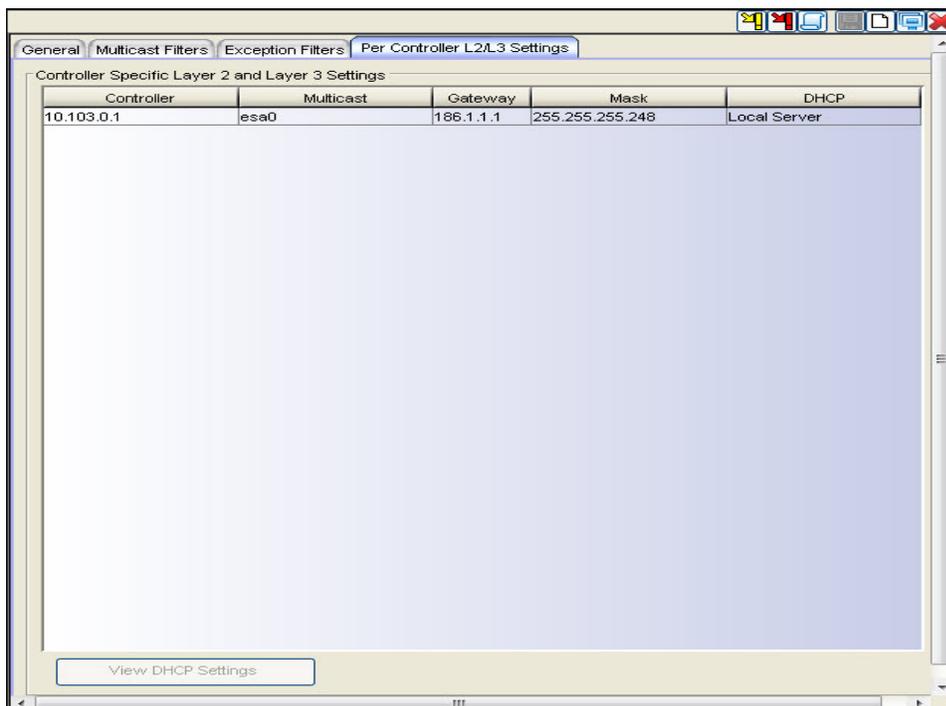
The following list describes the information available on the Per Controller L2/L3 Settings tab.

Controller
Wireless Controller to which the group of settings in the table row applies.

Gateway
The Wireless Controller's IP address on the topology (VLAN).

Mask
Mask - The subnet mask that applies to traffic on the topology (VLAN) at the Wireless Controller.

DHCP
Specifies whether DHCP is enabled on the EWC for this topology and if so, whether DHCP relay or DHCP server mode is in effect.

View DHCP Settings
Click to view DHCP settings.

Mode
If the DHCP mode is "DHCP relay" then this attribute will be displayed. It is the IP address of the DHCP server to which the DHCP relay will forward DHCP traffic.

Domain Name
The domain name that DHCP clients should use.

Lease (seconds) default
The time period for which the IP address will be allocated to any device requesting it.

Lease (seconds) max
The maximum time period in seconds for which the IP address will be allocated to any device.

DNS Servers
IP address of DNS servers. This list will be sent to DHCP clients along with an IP address.

WINS
IP address of WINS servers. This list will be sent to DHCP clients along with an IP address.

DLS Address

The address of a maintenance server. This setting is sent to Siemens Enterprise WL2 phones. To provide the address of the DLS server, first check the "Enable DLS DHCP option" checkbox, then supply an address in the DLS address field.

Next Hop Address

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.

OSPF Route Cost

Enter the OSPF cost of reaching the VNS subnet. This value provides a relative cost indication to allow upstream routers to calculate whether or not to use the Wireless Controller as a better fit or lowest cost path to reach devices in the network.

Address Range

The first and last address in the range of addresses that the DHCP server can give out for this topology.

Exclusions

Click this button to be able to specify one or more ranges within the overall address range that should not be given out.

B'cast Address

This field populates automatically based on the IP address and subnet mask of the VNS.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

NOTE: It will only be possible to delete a topology if it is not in use by Policy Manager or referenced by another template.

Viewing Topology Summary Information

You can view summary information for all topologies discovered on Wireless Controllers or created in Wireless Manager. This information is available from the Topologies Summary page. You can display this information by topology name or topology type.

From the Topology Summary page, you can also perform the following tasks:

- Retrieve the list of topologies associated with all managed Wireless Controllers.

- Deploy or undeploy the topology.

- Edit or clone an existing topology.

- Export the configuration to the Wireless Controller's CLI.

- Create a new topology.

- Delete an existing topology.

To view the Topologies Summary page:

1. Click the Configured Objects tab.

2. In left-hand pane, click Network Topologies. The Network Topologies Summary page displays.

The following list describes the information available on the Network Topologies Summary Page.

Status

Status of this Network Topology. Options include:

○ Deployed, ○ Not Deployed, ⊘ Deployed but not synchronized to the network

Topology Name
A string of alphanumeric characters used to identify the topology.

Group
Indicates whether the topology is part of a topology group. Options include:

✓ Included in a topology group, ✗ Not included in a topology group

VID
The VLAN identifier as specified in the IEEE 802.1Q definition.

Tagged
Indicates whether the VLAN is tagged or untagged.

Type
Indicates the type of topology. Options include:

Routed

B@AP (Bridged @ AP)

B@HWC (Bridged @ Controller)

No. Controllers
Number of Wireless Controllers using this topology.

Controllers
For topologies corresponding to PM VLANs, 'Controllers' lists by IP address those controllers in the PM domain. For topologies which have no VLAN counterpart in PM, 'Controllers' lists by IP address those controllers to which the topology has been deployed.

Toolbar Buttons
For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

NOTE: It will only be possible to delete a topology if it is not in use by Policy Manager or referenced by another template.

Editing a Topology

You can edit a topology at any time. Any changes that you make to a topology configuration do not take effect until you create a task to deploy the modified topology.

To edit a topology:

1. Click the Configured Objects tab.

2. In left-hand pane, click Network Topologies. The Network Topologies Summary page displays.

3. Select a topology on the Topologies Summary page and either click the edit icon at the top of the page or right-click on the task name and select Edit from the drop-down menu. The Topologies Summary page displays.

Deleting a Topology

You can delete a topology only if it is not currently being used or referenced by a role, WLAN, or topology group. Deleting a topology group deletes only that topology group, not the topologies it contains.

To delete a topology:

1. Click the Configured Objects tab.

2. In left-hand pane, click Network Topologies. The Network Topologies Summary page displays.

3. Select a topology from the list on the Topologies Summary page.

4. Click the Delete icon. Wireless Manager prompts to verify that you want to delete the selected topology.

5. Click **OK** to continue or **Cancel** to abort the topology deletion.

About Wireless Networks in Extreme Management Center (Legacy)

Using the Wireless Networks tab in Wireless Manager, you can view information about elements of your wireless network, including Wireless Controllers, Mobility Zones, and shared secrets.

This Help topic includes the following information:

- [Shared Secrets Page](#)
- [Viewing Mobility Zone Summary Information](#)
- [Viewing Mobility Zone Details](#)
- [Viewing Controller Summary Information](#)
- [Viewing Controller Details](#)
- [Adaptive Management UI](#)
    - [Browser Certificate Warnings](#)
    - [Accessing the Dashboard Page](#)
    - [Accessing the Logs Page](#)
    - [Accessing the Wireless Controller Configuration Page](#)
    - [Accessing the Wireless APs Page](#)
    - [Accessing the VNS Configuration Page](#)

Shared Secrets Page

Wireless Manager relies on shared secrets for authentication with Wireless Controllers. From the Generate Shared Secrets page, you can set the shared secret used to authenticate Wireless Manager to a Wireless Controller and you can change that shared secret manually or by generating a random shared secret.

You can view the shared secret for each Wireless Controller from the Wireless Controller summary page and from the Wireless Controller configuration page.

To set the shared secret used with a Wireless Controller:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Generated Shared Secrets. The Generate Shared Secret page displays.
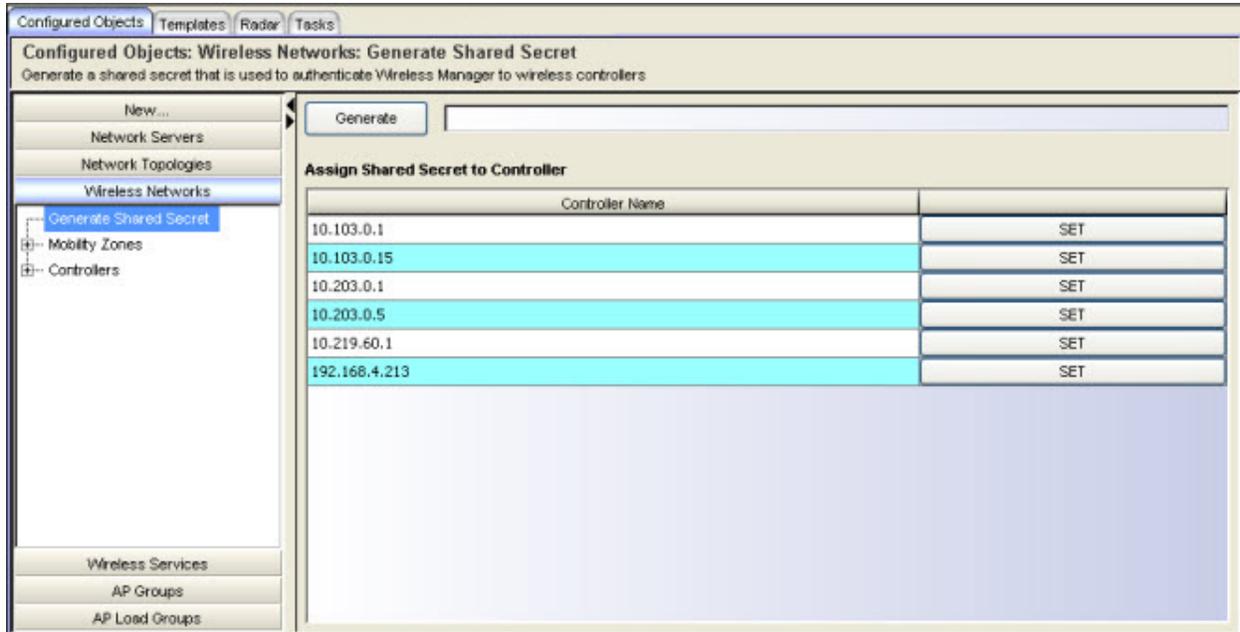
The following list describes the information available on the Generate Shared Secret page.

Generate

Click to generate a random shared secret. The shared secret displays in the empty field.

Controller Name

The name or IP address of the Wireless Controller.

Set

Click to assign the generated shared secret to the corresponding Wireless Controller.

Viewing Mobility Zone Summary Information

A Mobility Zone is a set of Wireless Controllers organized in a logical pattern so that a mobile user can seamlessly roam between the APs of different Wireless Controllers in the set. A Mobility Zone can only be configured from the Wireless Controller (for more information, refer to the *Extreme Networks Wireless Convergence Software User Guide* for details on setting up a Mobility Zone). A

Mobility Zone may contain up to 12 controllers; one controller in the group is designated as the mobility manager, and all others are designated as mobility agents.

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 the registration behavior for a multi-controller mobility domain.
- 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.

A controller designated as a mobility agent:

- 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 the connection to 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 the connection to 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.

In Wireless Manager, a Mobility Zone is created when a Wireless Controller that is the manager for a Mobility Zone is managed by NetSight. The Mobility Zone is maintained until that Wireless Controller is unmanaged.

To view the Wireless Controllers assigned to each Mobility Zone:

1. Click the Configured Objects tab.
2. In left-hand pane, click Wireless Networks > Mobility Zones. The Mobility Zones page displays.
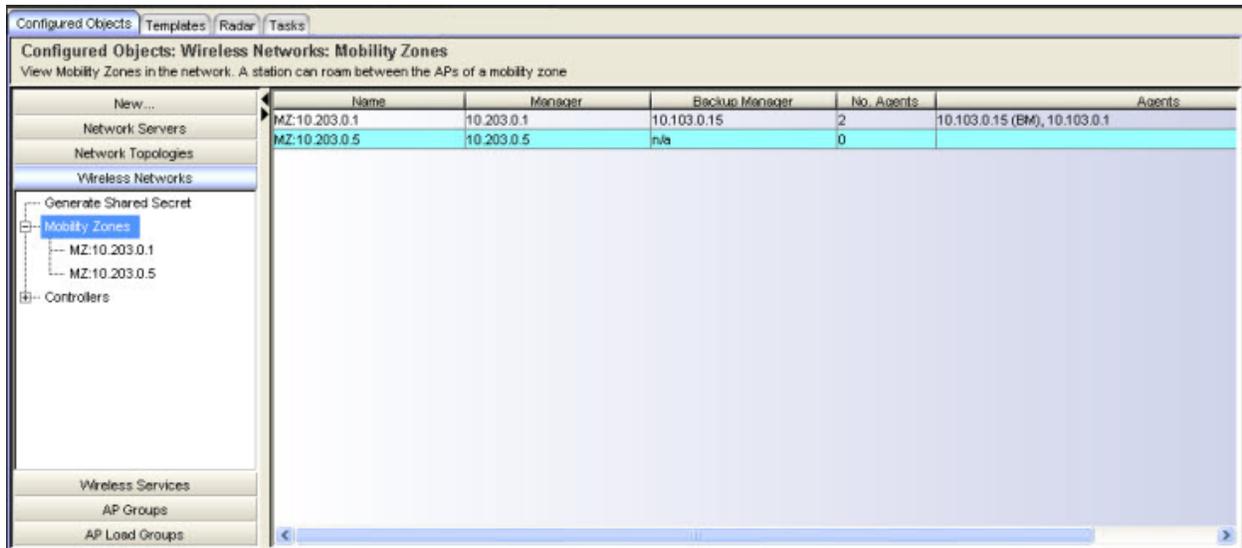
The following list describes the information available on the Mobility Zones Summary page.

Name
Mobility Zones are named according to the IP address of their Manager Wireless Controller.

Manager
IP address of the manager of the Mobility Zone.

Backup Manager
IP Address of the VN backup manager. In the event that the primary VN manager crashes, the backup VN manager takes over responsibility for 1) distributing MU sessions to the other VN agents in the mobility domain, and 2) helping to setup data & controller tunnels in the mobility domain. Only one manager is active at a time, the other works as a normal VN agent in PASSIVE mode. When both the primary and backup managers are active, the primary manager will assume the role of VN manager.

No. Agents
Number of agents that are part of this Mobility Zone.

Agents
List of IP addresses of the Mobility Zone agent Wireless Controllers. The agent configured as the backup manager will be displayed with a "(BM)" next to its display name.

Viewing Mobility Zone Details

To view detailed information about a particular Mobility Zone:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Mobility Zones. The Mobility Zones Summary page displays.

3. Click on a Mobility Zone in the list. The Mobility Zones Details page displays.

The following list describes the information available on the Mobility Zones Details page.

Manager
IP address of the manager of the Mobility Zone.

Mgmt MAC Address
MAC address of the selected manager Wireless Controller.

Version
The software version running on the manager Wireless Controller.

Agent
List of IP addresses of the Mobility Zone agent Wireless Controllers.

Mgmt MAC Address
MAC address of the selected agent Wireless Controller.

Version

The software version running on the selected agent Wireless Controller.

Viewing Controller Summary Information

You can view summary information about all Wireless Controllers known to Wireless Manager from the Wireless Controllers Summary page. From this page, you can also:

- Connect to the ExtremeWireless Wireless Assistant to modify Wireless Controller settings.

- Connect to Management Center to view reports and statistics.

- Select a Wireless Controller and click the edit icon to view the collected Wireless Controller details and to edit the Wireless Controller's shared secret.

To view Wireless Controller summary information:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers. The Wireless Controllers Summary page displays.

The following list describes the information available on the Controllers Summary page.

IP Address

IP address assigned to the selected Wireless Controller.

Host Name

Name assigned to the selected Wireless Controller.

Mgmt MAC Address

MAC address of the selected Wireless Controller.

Version

The software version running on the selected Wireless Controller.

Shared Secret

Shared secret used for communication between the Wireless Controller and Wireless Manager.

Sync Status

Synchronization status which identifies whether Wireless Manager was able to read relevant configuration data from the Wireless Controller.

AP Name

Names of the APs associated with the selected Wireless Controller.

AP Role

Role of the AP in the network.

Location

Location of the AP. Options include Foreign or Local.

Status

Approval status of the AP.

Active

Current activity status of the AP. Options include Active or Inactive.

IP Address

IP address assigned to the selected AP.

MAC Address

MAC address of the selected AP.

Hardware Type

Hardware model of the selected AP.

Toolbar Buttons

For a description of common toolbar buttons see <u>Context-Sensitive Toolbar</u>.

Viewing Controller Details

To view detailed information about a particular Wireless Controller:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers. The Controller Summary page displays.

3. Click on a Wireless Controller in the list. The Wireless Controller Details page displays.
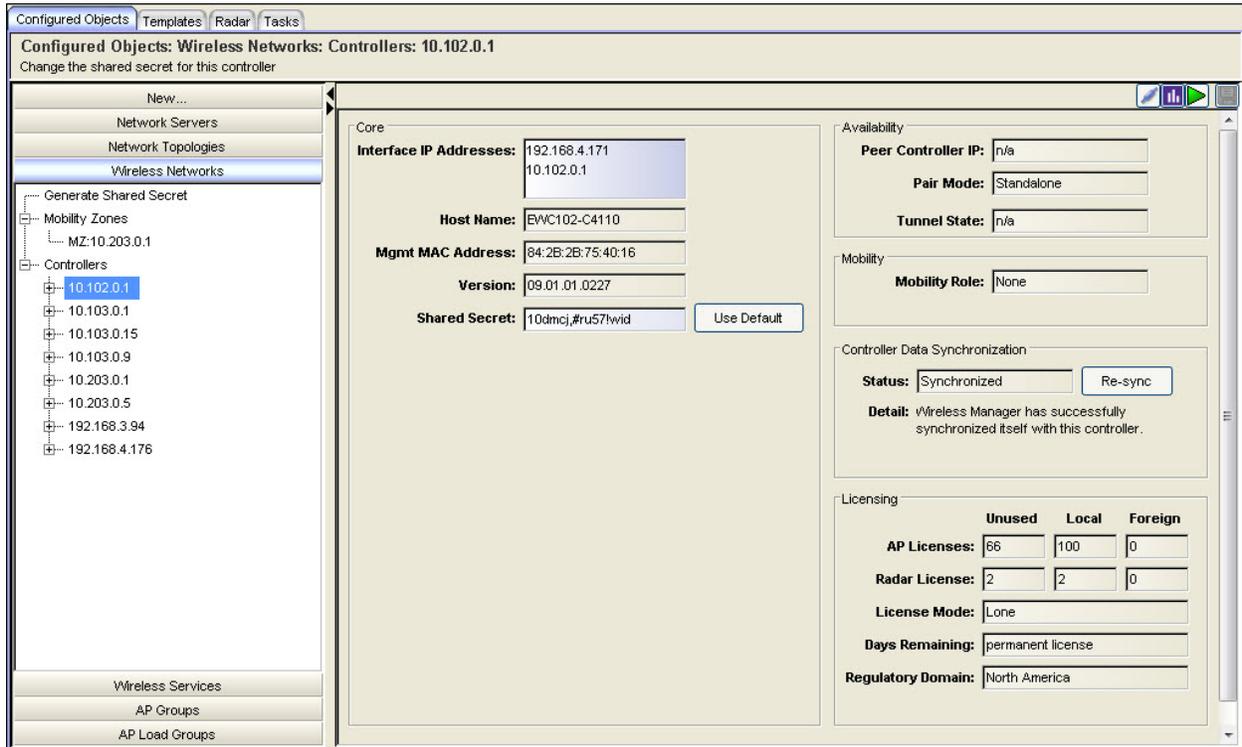
The following list describes the information available on the Controller Details page.

Core

Interface IP Addresses
The IP addresses associated with the physical topologies (including Admin) of the Wireless Controller.

Host Name
Name assigned to the selected Wireless Controller.

Mgmt MAC Address
MAC address of the selected Wireless Controller.

Version
The software version running on the selected Wireless Controller.

Shared Secret

Shared secret used for communication between the Wireless Controller and Wireless Manager.

Availability

Peer Controller IP

MAC address of the selected Wireless Controller. If the Wireless Controller is a part of an availability peer, this is the availability peer's IP address.

Pair Mode

Identifies whether the Wireless Controller is part of an availability pair or is a standalone Wireless Controller.

Tunnel State

Displays the state of the data tunnel between Wireless Controllers.

Mobility

Mobility Role

Role that the Wireless Controller takes in a Mobility Zone. Options include: Agent or Manager.

Controller Data Synchronization

Status

Status that identifies whether Wireless Manager is able to read relevant configuration information from the Wireless Controller. Possible values are:

Not synchronized - Wireless Manager cannot read relevant configuration data from the Wireless Controller.

Synchronized - Wireless Manager can read relevant configuration data from the Wireless Controller.

Detail

An informational message that identifies the reason why the status is Not Synchronized.

Licensing

AP Licenses

Displays the following AP license information:

Unused AP Licenses: Total number of unassigned AP licenses.

Local AP Licenses: Total number of AP licenses local to this controller.

Foreign AP Licenses: Total number of AP licenses local to this controller's availability partner.

Radar Licenses

Displays the following Radar license information:

Unused Radar Licenses: Total number of unassigned Radar licenses.

Local Radar Licenses: Total number of Radar licenses local to this controller.

Foreign Radar Licenses: Total number of Radar licenses local to this controller's availability partner.

A Radar capacity license is required for APs assigned to In-Service and Guardian scan profiles. Each assigned AP counts as one against the licensed Radar capacity.

If the number of APs licensed for Radar is zero, you can create a scan profile without assigned APs, update a scan profile but only remove assigned APs, or delete a scan profile.

License Mode

Displays the license mode for the selected controller. A controller can operate in either Lone or Paired mode.

Lone (standalone) - Only local APs are counted against locally installed AP capacity keys. All Radar In-Service and Guardian APs are counted against locally installed Radar keys. This is the default license mode. A controller switches to Paired mode when Availability is enabled.

Paired - Both local and foreign APs are counted against the sum of locally installed AP capacity keys and AP capacity keys pooled from the peer controller. All Radar In-Service and Guardian APs are counted against the sum of Radar keys installed locally and on the peer controller. A controller switches to Lone (standalone) mode if Availability is disabled.

Days Remaining

Displays the number of days remaining on this license key. When an evaluation license or grace period (for installing the appropriate major release key) expires, all Radar functions stop until a permanent license is installed.

Regulatory Domain

Displays the regulatory domain for which the controller is licensed.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Adaptive Management UI

You can view configuration and summary information about a specific Wireless Controller, running V8.11 or later, using the Adaptive Management User Interface (UI). Once synchronized, Wireless Manager retrieves Wireless Controller management UI data and displays the menu hierarchy under Configured Objects > Wireless Networks > Controllers > specific Wireless Controller.

The adaptive management menu is intended to allow Wireless Manager to be able to easily configure all aspects of 8.11+ Wireless Controllers. Wireless Manager can also support the configuration of a Wireless Controller running software released after Wireless Manager was released, by retrieving its management menu each time the controller transitions to Synchronized.

Although the adaptive management menu may be different for different Wireless Controller versions, in general, its structure mirrors the menu hierarchy of the Wireless Controller that reported it, except for those menu items which refer to features of the Wireless Controller which are already configurable by Wireless Manager. For example, Wireless Manager purposefully excludes the following menu items under VNS Configuration, from each Wireless Controller's adaptive management menu: Global > Bandwidth Control, Virtual Networks, WLAN Services, Policies, Class of Services, and Topologies.

Clicking a menu item launches the default browser which displays the corresponding controller page (in either a new window or new tab). This browser window simplifies your navigation within and between the pages of the various controller GUIs, by including on the left-hand side of the page all discovered controllers and their adaptive management menus. The menus are identical to those displayed in Wireless Manager's Configured Objects > Wireless Networks > Controllers submenu, except that clicking a menu item opens the corresponding controller page on the right-hand side without opening a new browser window.

The adaptive management feature is only available to users with Wireless Manager Configure capability.

The following top-level Wireless Controller pages are accessible using the Adaptive Management UI:

- [Dashboard](#)
- [Logs](#)
- [Wireless Controller](#)

- [Wireless APs](#)
- [VNS Configuration](#)

Browser Certificate Warnings

Certificate related warnings may appear when clicking links in the adaptive management menu for a Wireless Controller. Instructions provide steps on how to handle each warning based on the following types (and versions) of browsers:

- [Chrome](#)
- [Firefox](#)
- [Internet Explorer](#)

Chrome

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, select a Wireless Controller, and click the Connect button . The following error message displays on a blank page.
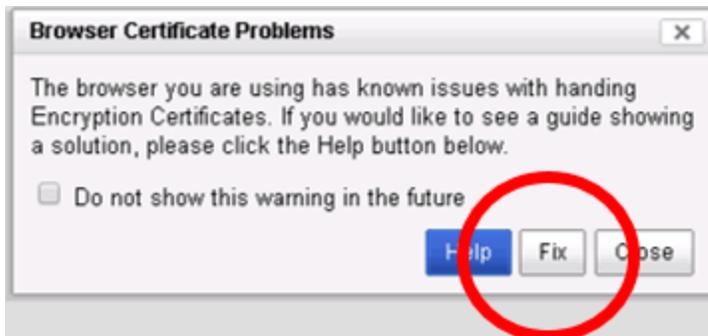
3. Click the **Fix** button. A dialog box appears informing you a new window will open.
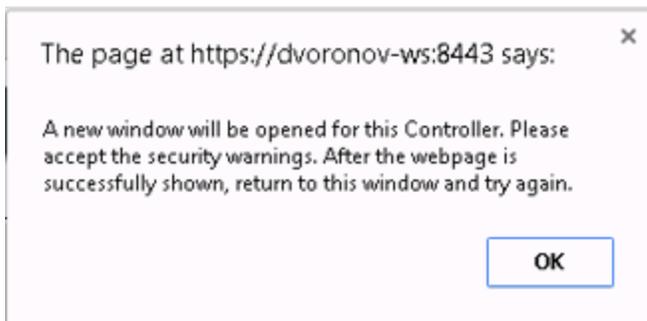
4. Click **OK**.

5. Click **Proceed to *IP* (unsafe)** when the following window is displayed.

6. Go to [Accessing the Dashboard Page](#).

Firefox

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, select a Wireless Controller, and click the Connect button ◨. The following error message displays.
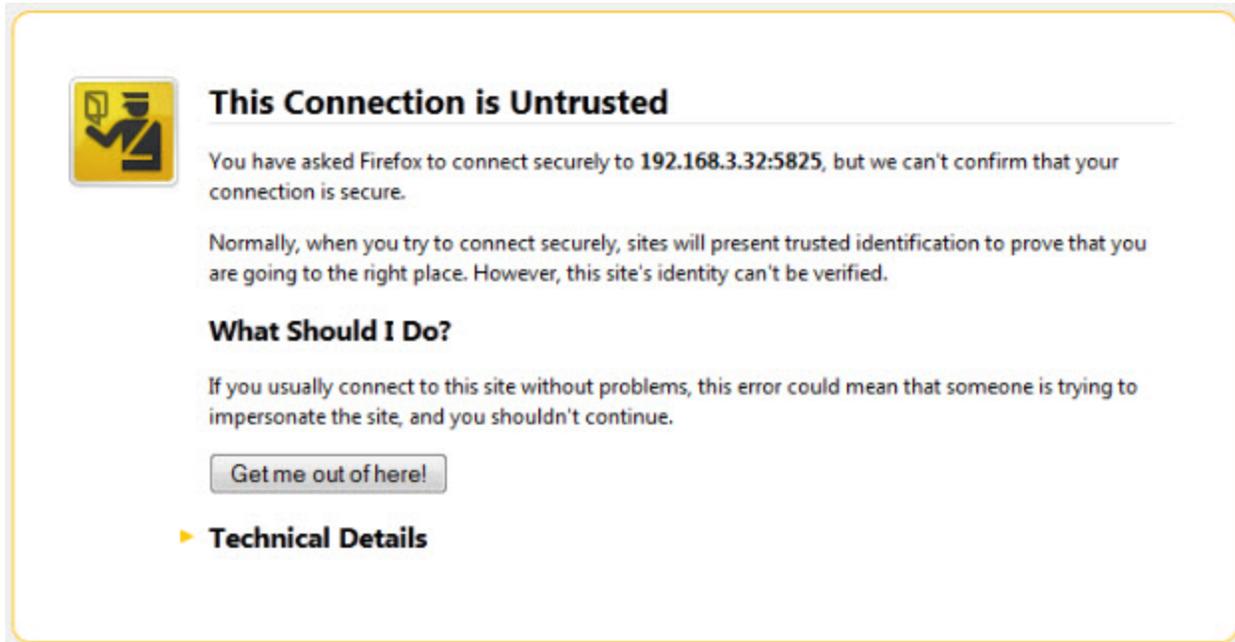
3. Right-click the error message, and select **This Frame** -> **Show Only This Frame**.
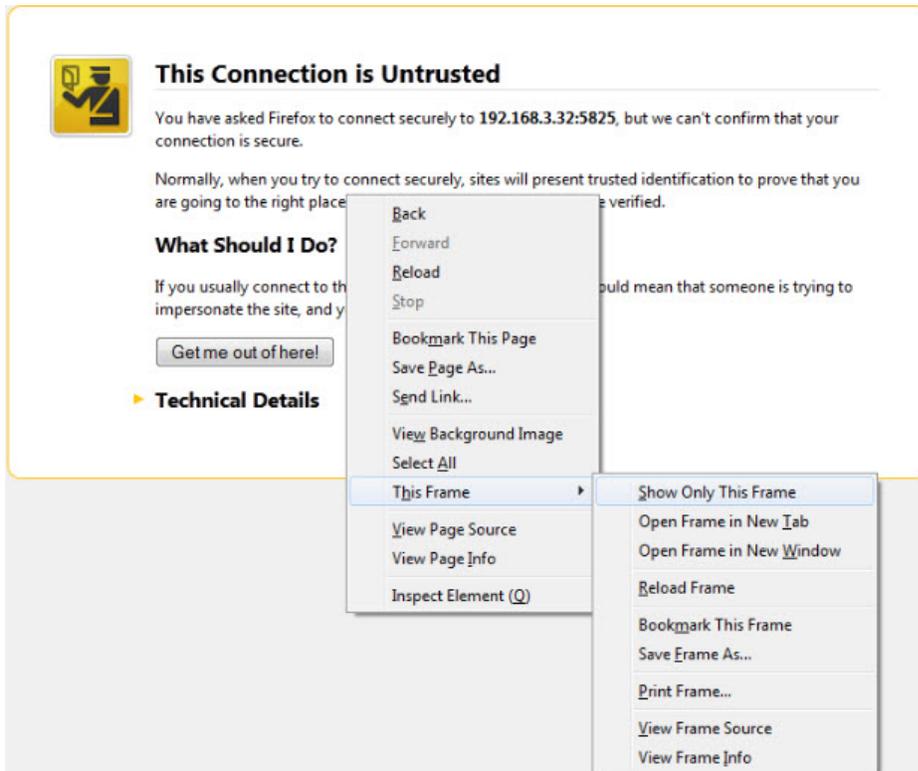
4. On the Untrusted dialog, click **Add Exception**.

5. On the Add Security Exception dialog, click **Confirm Security Exception**.
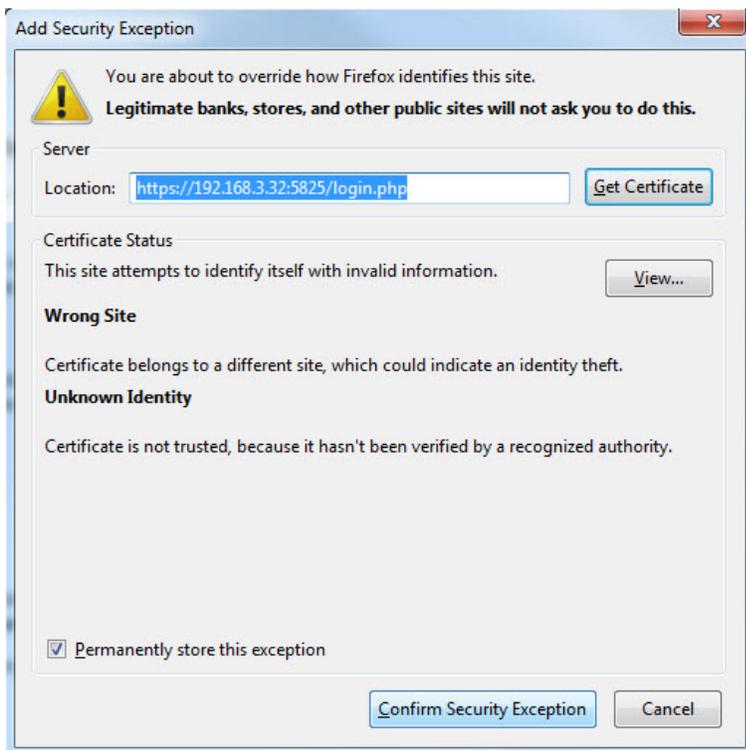
6. Click back.

7. Go to [Accessing the Dashboard Page](#).

Internet Explorer

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, select a Wireless Controller, and click the Connect button ⬚. The following error message displays.

> Content was blocked because it was not signed by a valid security certificate.
>
> For more information, see "About Certificate Errors" in Internet Explorer Help.

3. Click **Show content** at the bottom of the dialog.

> Internet Explorer blocked this website from displaying content with security certificate errors.   Show content   ✕

4. Go to [Accessing the Dashboard Page](#) .

Accessing the Dashboard Page

The Dashboard page (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).

To access the Dashboard page:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, and select a Wireless Controller. The tree node expands and displays the Wireless Controller menus.

3. In the left-hand pane, click Dashboard > Home. The Wireless Assistant Home page displays.

Accessing the Logs Page

The Wireless Assistant - Logs & Traces page contains messages that include 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, and login logs.

To access the Logs & Traces page:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, and select a Wireless Controller. The tree node expands and displays the Wireless Controller menus.

3. In the left-hand pane, click Logs. The Wireless Assistant Logs & Traces page displays.

Accessing the Wireless Controller Configuration Page

The Wireless Assistant - Wireless Controller Configuration page include a series of configuration tasks. These tasks include:

- Changing the administrator password
- Applying product license keys
- Setting up the data ports
- Setting up static routes

To access the Wireless Controller Configuration page:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, and select a Wireless Controller. The tree node expands and displays the Wireless Controller menus.

3. In the left-hand pane, click Wireless Controller. The Wireless Controller Configuration page displays.
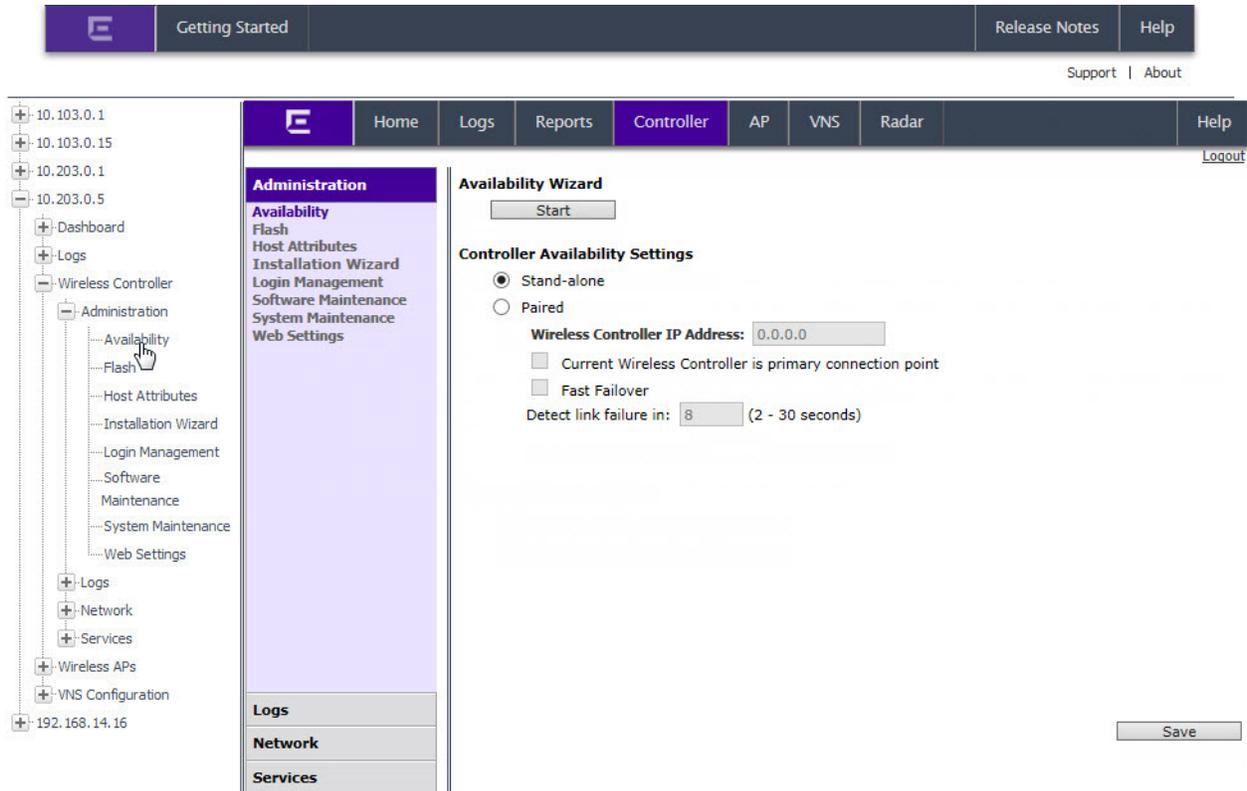
Accessing the Wireless APs Page

The Wireless Assistant - Wireless APs page includes menus that include information on how to install the wireless AP, how it discovers and registers with the Wireless Controller, and how to view and modify radio configuration.

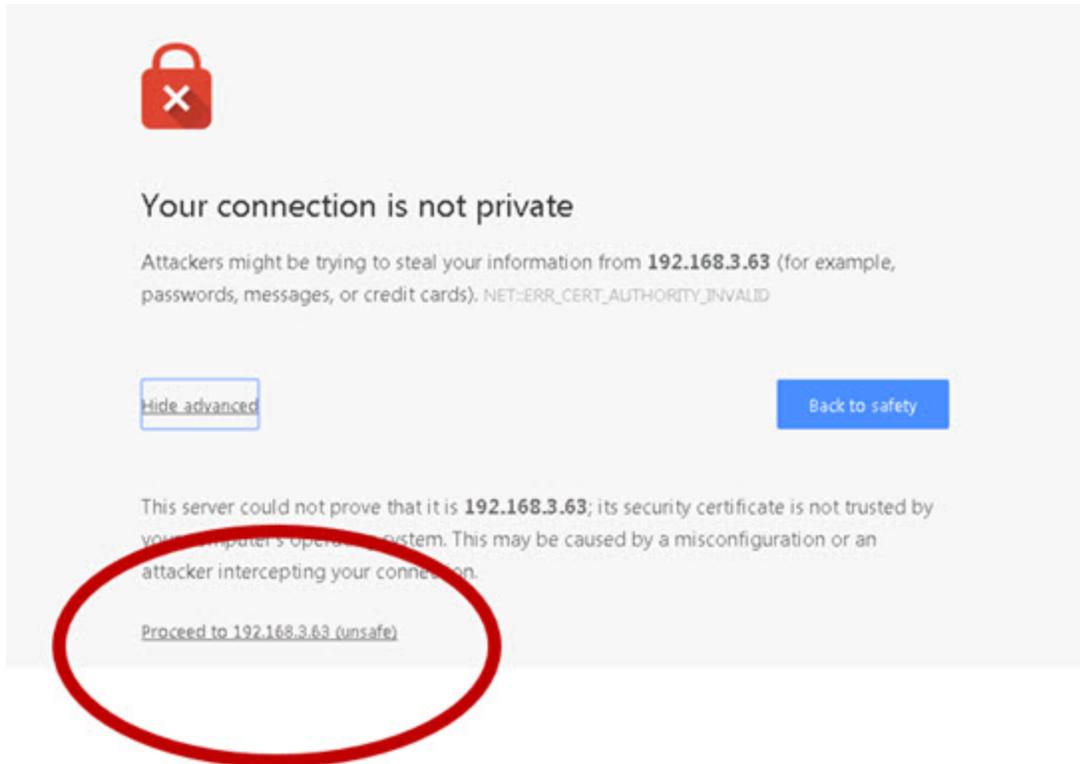To access the Wireless APs page:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, and select a Wireless Controller. The tree node expands and displays the Wireless Controller menus.

3. In the left-hand pane, click Wireless APs. The Wireless APs page displays.

IMPORTANT: NetSight version 8.0 supports up to 7,500 APs and 50,000 clients across all managed wireless controllers. For sites with more than the supported number of APs and clients, contact your sales representative to acquire an additional NetSight license.

Accessing the VNS Configuration Page

The Wireless Assistant - VNS Network Configuration page includes menus that provide detailed information on how to configure a VNS, either using the wizards or by manually creating the component parts of a VNS.

To access the VNS Network Configuration page:
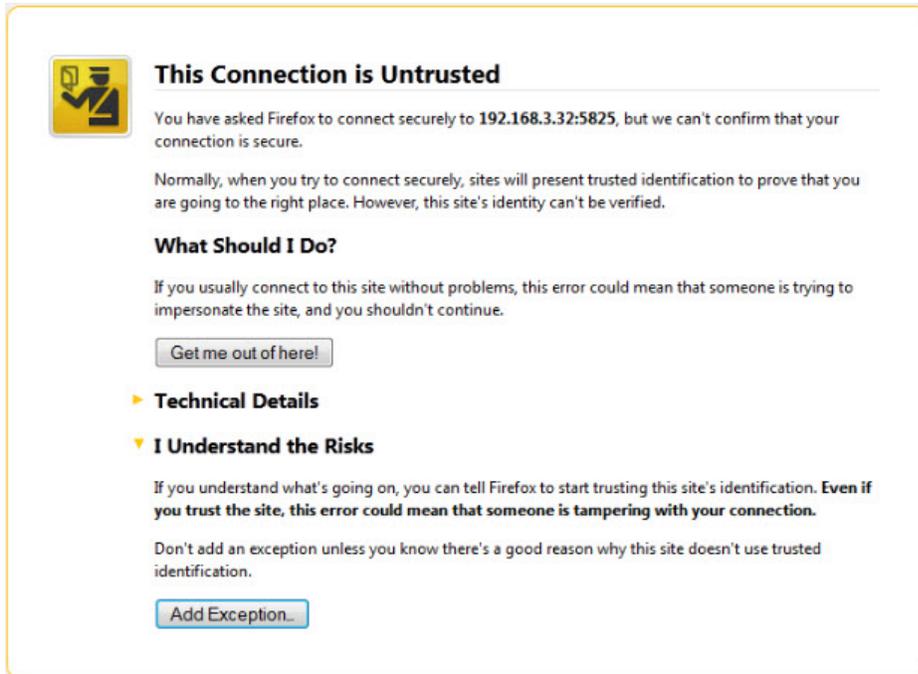
1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Networks > Controllers, and select a Wireless Controller. The tree node expands and displays the Wireless Controller menus.

3. In the left-hand pane, click VNS Configuration. The Virtual Network Configuration page displays.

About Wireless Services in Extreme Management Center (Legacy)

Service Set Identifiers (SSIDs) identify WLAN Services so that wireless devices can associate to them. When you discover Wireless Controllers, you also discover the Wireless Controllers' SSIDs.

> **NOTE:** Different WLAN services on different Wireless Controllers can have the same SSID.

This Help topic includes the following information:

- [Viewing the Discovered SSIDs](#)
- [Viewing Detailed Information About SSIDs](#)

Viewing the Discovered SSIDs

The SSIDs Summary page displays information about all discovered SSIDs.

To view the SSIDs discovered during Wireless Controller discovery:

1. Click the Configured Objects tab.

2. In left-hand pane, click Wireless Services. The SSIDs Summary page displays information about each of the SSIDs in the discovered portion of your wireless network.

The following list describes the information available on the SSIDs Summary page.

SSID Name
The SSID that identifies the service for wireless devices.

No. VNS
Number of different VNSs identified by this SSID.

Associated VNS's
Names of the VNS's associated with this SSID.

No. AP
The number of APs advertising this SSID.

Viewing Detailed Information About SSIDs

The SSID Details page displays detailed information about a selected SSID.

To view detailed information about a selected SSID:

1. Click the Configured Objects tab.

2. In the left-hand pane, click Wireless Services. The SSIDs Summary page displays.

3. Select an SSID from the list. The SSIDs Details page displays. To determine which APs are serving the SSID for a specific VNS, select the VNS on the left side of the table.
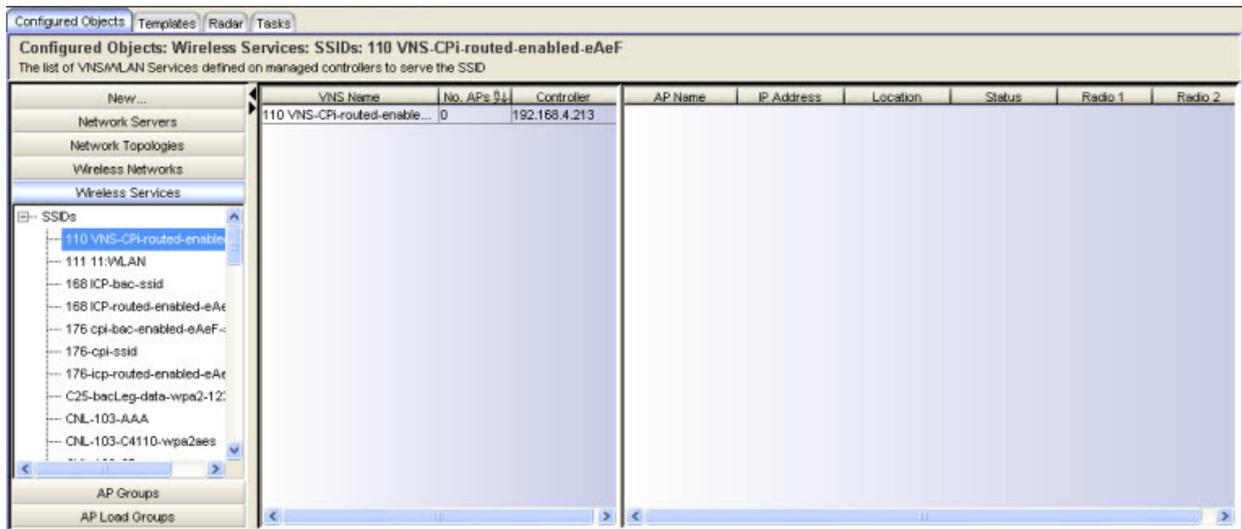
The following list describes the information available on the SSIDs Details page.

VNS Name

Name of the VNS associated with the SSID.

No. APs

Number of APs associated with the Wireless Controller.

Controller

IP address of the Wireless Controller hosting the VNS.

AP Name

Names of the APs advertising the SSID on behalf of the selected VNS.

IP Address

IP address of the AP.

Location

AP location. Options are: Local or Foreign.

Status

Connection status of AP (Active or Inactive).

Radio 1

Radio 1 configuration setting.

Radio 2

Radio 2 configuration setting.

About AP Groups in Extreme Management Center (Legacy)

An AP Group is a named collection of APs. The APs in the AP Group can belong to different Wireless Controllers. You can use an AP Group as you would an individual AP so that you can apply the same configuration settings to multiple APs at the same time.

Wireless Manager automatically creates a Default AP Group for each managed Wireless Controller. This Default AP Group contains all of the APs that have been approved as local APs and that have been reported as active on the Wireless Controller at least once. This per-controller Default AP Group includes all APs associated with the specified Wireless Controller.

You can also create additional AP Groups called Custom AP Groups. Any AP known to Wireless Manager can be added to any Custom AP Group and an individual AP can be included in more than one AP Group.

This Help topic includes the following information:

- [Viewing a List of AP Groups](#)
- [Viewing AP Groups Details](#)
- [Creating an AP Group](#)
- [Editing an AP Group](#)
- [Deleting an AP Group](#)

Viewing a List of AP Groups

To view a list of AP Groups configured in Wireless Manager:

1. Click the Configured Objects tab.
2. In left-hand pane, click AP Groups.
3. The AP Groups Summary page displays. The page lists characteristics about all defined AP Groups. To create a new AP Group, refer to [Creating an AP Group](#). To change an existing AP Group, refer to [Editing an AP Group](#).
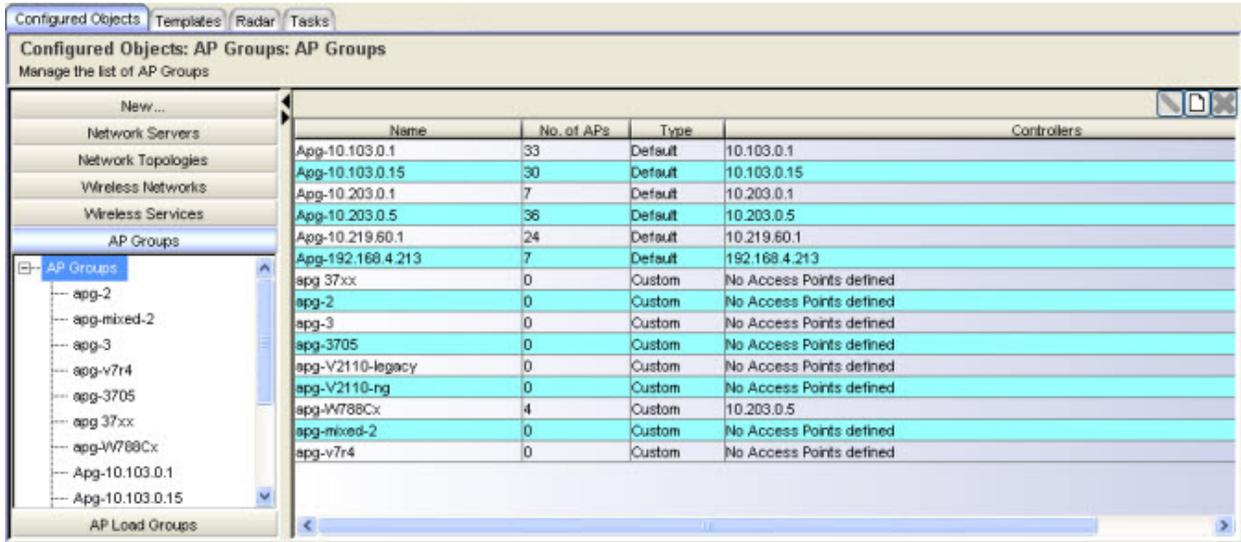
The following list describes the information available on the AP Groups Summary page.

Name

Name assigned to the AP Group.

No. of APs

Number of APs assigned to the AP Group.

Type

Identifies whether the AP Group is a Default AP Group or a user-created Custom AP Group.

Controllers

Names of the Wireless Controllers associated with the APs included in the AP Group.

Toolbar Buttons

For a description of common toolbar buttons see Context-Sensitive Toolbar.

Viewing AP Groups Details

To view detailed information about a particular AP Group:

1. Click the Configured Objects tab.

2. In left-hand pane, click AP Groups. The AP Groups Summary page displays.

3. Double click on the name of an AP Group listed under AP Groups. The AP Group Details page displays.
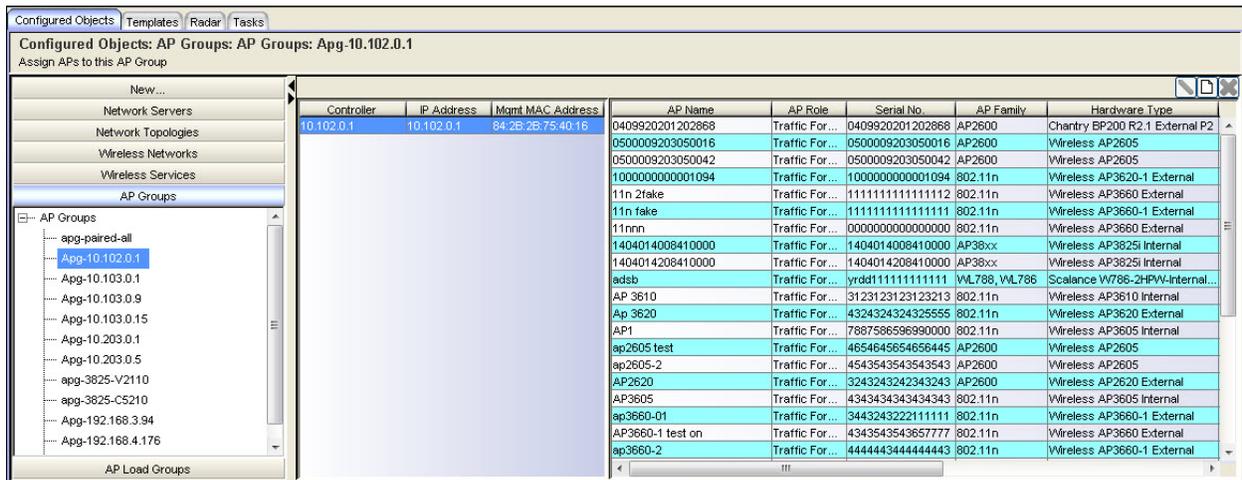
The following list describes the information available on the AP Groups Details page.

Controller
The display name of the Wireless Controller.

IP Address
IP address of the Wireless Controller associated with the AP Group.

Mgmt MAC Address
The MAC address of the Wireless Controller's management port. The controller software activation licenses are locked to this address.

AP Name
Name of the AP included in the AP Group.

AP Role
Role of the AP in the network.

Serial No.
Serial number of the AP.

AP Family
Model family of the AP.

Hardware Type
Specific hardware type of the AP.

Controller
The IP address of the Wireless Controller that the specified AP is associated.

Status

Approval status of the AP.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Creating an AP Group

To create an AP Group, you must select APs from the list of all controller-managed APs known to Wireless Manager. After you create the AP Group, Wireless Manager generates an audit record that shows the name of the AP Group, the user ID of the account that created the AP Group, and the date and time when it created the AP Group.

To create an AP Group:

1. Click the Configured Objects tab.
2. In left-hand pane, click AP Groups. The AP Groups Summary page displays.
3. Click on the New icon in the tool bar. The Create New AP Group page displays.

4. In the AP Group Name field, enter the name of the new AP Group.
5. In the WLAN Controller field, click on a controller name. When you select a controller, the list of APs associated with that controller populate the Available APs window.

6. To include an AP in the named AP Group, select an AP from the Available APs window and use the right arrow key to move it into the APs in Group window. To remove an AP from the named AP Group, select an AP in the APs in Group window and use the left arrow key to move it into the Available APs window.

7. To create an AP Group that contains APs from multiple Wireless Controllers, select another controller from the WLAN Controller list and repeat steps 5 and 6.

8. Click **OK** to save the new AP Group or click **Cancel** to discard the AP Group configuration.

You can also access the Create New AP Group page from the Configured Objects tab by clicking New > AP Group or from the AP Group Summary page by right-clicking on a controller name and selecting the New icon.

Editing an AP Group

You can edit only user-created Custom AP Groups; you cannot edit Default AP Groups.

To edit a Custom AP Group configuration:

1. Click the Configured Objects tab.

2. In left-hand pane, click AP Groups. The AP Groups Summary page displays.

3. Select an AP Group from the list on the AP Groups Summary page.

4. Click the Edit icon. The Edit AP Group page displays.
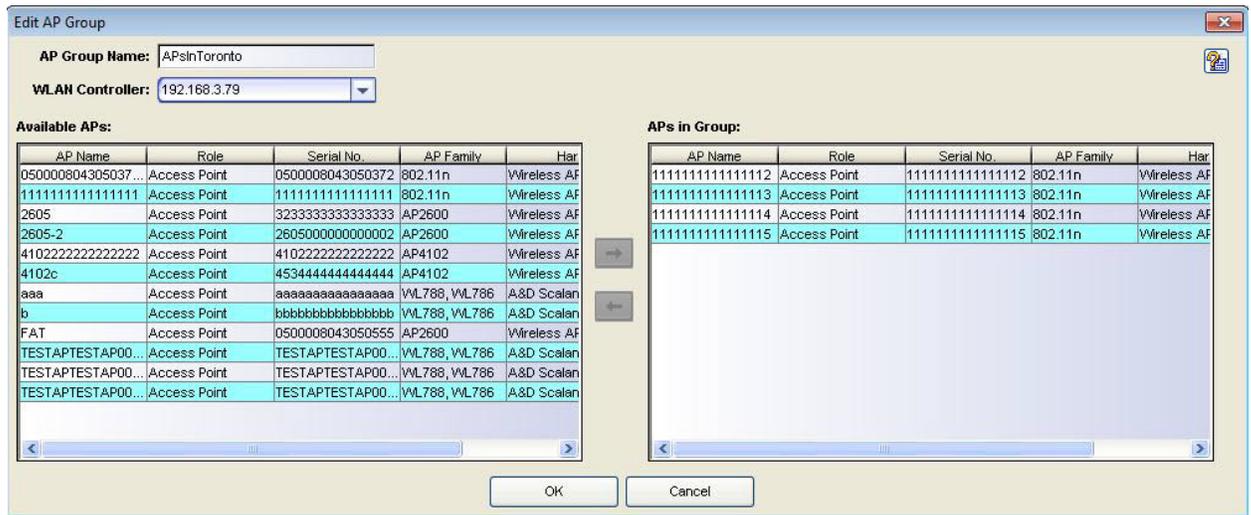
5. You can change the WLAN controller and the APs included in the AP Group.

6. Click **OK** to save the changes; click **Cancel** to discard the changes.

Deleting an AP Group

You can delete only user-created Custom AP Groups; you cannot delete Default AP Groups.

To delete an AP Group configuration:

1. Click the Configured Objects tab.

2. In left-hand pane, click AP Groups. The AP Groups Summary page displays.

3. Select an AP Group from the list on the AP Groups Summary page.

4. Click the Delete icon. Wireless Manager prompts to verify that you want to delete the selected AP Group.

5. Click **OK** to continue or **Cancel** to abort the AP Group deletion.

You can also delete an AP Group from the AP Group Details page.

About AP Load Groups in Extreme Management Center (Legacy)

An AP Load Group is defined as a group of APs and their radios to which WLAN services can be assigned. There are two types of AP Load Groups:

- Client balancing - Distributes clients across multiple co-located APs covering one open area. An AP radio can only be in one Load Group. However, Wireless Manager can still assign a radio in multiple Load Groups as long as the Load Group template is not deployed to the Wireless Controller.
- Radio balancing - Manages the number of clients on a specific radio by disabling additional clients on the radio above the configured radio load. Radio balancing Load Groups force all radios of an AP be put in the Load Group.

This Help topic includes the following information:

- [Viewing the List of AP Load Groups](#)
- [Viewing AP Load Groups Details](#)
- [Creating an AP Load Group](#)
- [Editing an AP Load Group](#)
- [Deleting an AP Load Group](#)

Viewing the List of AP Load Groups

To view the list of AP Load Groups configured in Wireless Manager:

1. Click the Configured Objects tab.
2. In left-hand pane, click AP Load Groups.
3. The AP Load Groups Summary displays. The page lists information about each of the AP Load Groups defined on the Wireless Manager. To create a new AP Load Group, see [Creating an AP Load Group](#). To change an existing AP Load Group, see [Editing an AP Load Group](#).

The following list describes information available on the AP Load Groups Summary page.

Status

Status of this AP Load Group. Options include: ⊙ Deployed, ⊙ Not deployed, ⊘ Deployed but not synchronized to the network.

Name

Name assigned to the AP Load Group.

Controller

Name of the Wireless Controller associated with the APs included in the AP Load Group. The controller can be identified by an IP address or an alphanumeric string.

Group Type

Type of AP Load Group.

Num APs

Number of APs assigned to this AP Load Group.

Num WLANs

Number of WLANs assigned to this AP Load Group.

Toolbar Buttons

For a description of common toolbar buttons see Context-Sensitive Toolbar.

Viewing AP Load Groups Details

To view detailed information about a particular AP Load Group:

1. Click the Configured Objects tab.

2. In left-hand pane, click AP Load Groups. The AP Load Groups Summary page displays.

3. Double-click the name of an AP Load Group. The AP Load Groups Details page displays.
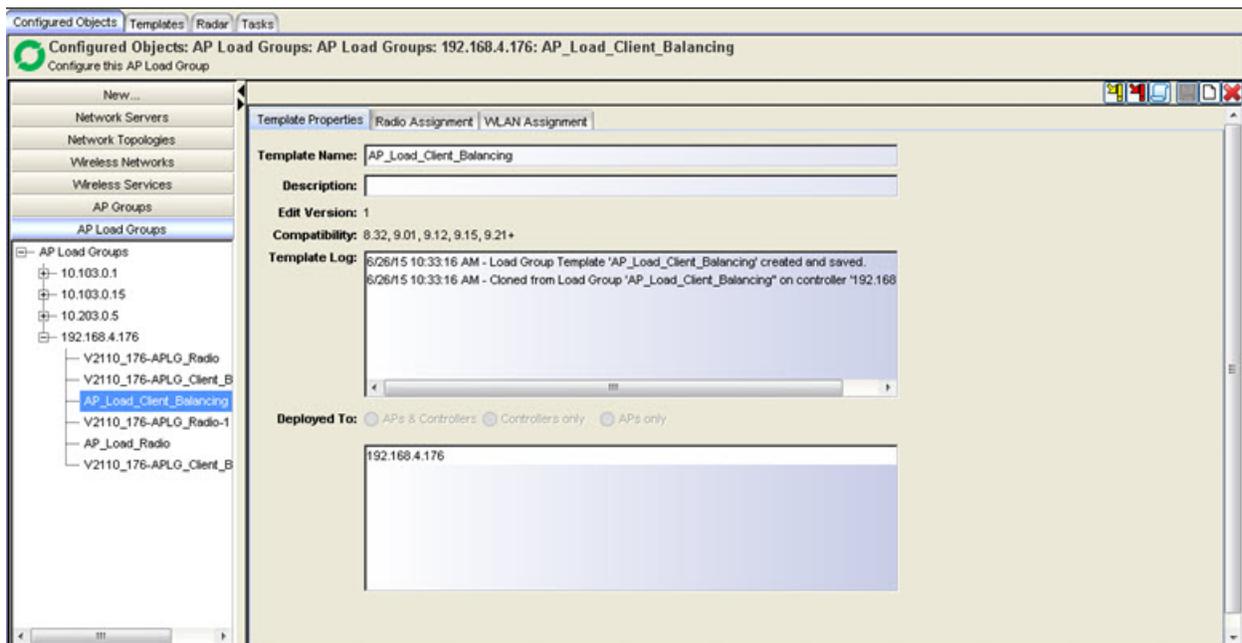
The following list describes information available on the AP Load Groups Details page.

Template Properties Tab

Template Name
Name of this template.

Description
Text used to describe the purpose of this Load Group.

Edit Version
Increments each time this template is edited.

Compatibility

Displays the versions of the Wireless Controller software that are compatible with this template (see Template Versions).

Template Log

The history lists significant events in the life of the template, such as when it was created, when it was changed, and when it was deployed.

Deployed to

Lists the Wireless Controllers to which this scan profile template is deployed.

Radio Assignment Tab

Load Group ID

Name of this Load Group.

Type

Type of Load Group. Set to Client Balancing.

Select AP radios

Select the radios assigned to this Load Group. Possible values are: All radios, Radio 1, Radio 2, Clear all Selections.

Controller

Name of the Wireless Controller assigned to this Load Group. Select a controller from the drop-down menu.

Radio Preference Tab

Load Group ID

Name of this Load Group.

Type

Type of Load Group. Set to Radio Balancing.

Controller

Name of the Wireless Controller assigned to this Load Group. Select a controller from the drop-down menu.

Band Preference

Select the checkbox to enable band preferences for this Load Group.

Load Control

Select the following parameters for each radio assigned to this load group:

- **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.

WLAN Assignment Tab

Template Name

Name of this template.

WLAN Name

Name of this WLAN.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Creating an AP Load Group

When creating an AP Load Group, you can only select APs/radios from a single Wireless Controller to become members of the group. After you create the AP Load Group, Wireless Manager generates an audit record that shows the name of the AP Load Group, the user ID of the account that created it, and the date and time when it was created.

To create an AP Load Group:

1. Click the Configured Objects tab.

2. In left-hand pane, click AP Load Groups. The AP Load Groups Summary page displays.

3. Click on the New icon in the tool bar. The AP Load Group Details page displays.

4. In the Template Name field, enter a name for the Wireless Controller.

5. In Description field, describe the purpose of this Load Group.

6. Click the Radio Assignment tab and enter the following information:

   - Enter a Load Group ID.

   - Select the Load Group Type.

   - Select a Wireless Controller from the list of available controllers.

   - Select AP radios.

7. Click the Save icon to save the AP Load Group configuration.

You can also access the Create New AP Load Group page from the Configured Objects tab by clicking New > AP Load Group or from the AP Load Group Summary page by right-clicking on a Wireless Controller name and selecting the New icon.

Editing an AP Load Group

To edit an AP Load Group configuration:

1. Click the Configured Objects tab.

2. In left-hand pane, click AP Load Groups. The AP Load Groups Summary page displays.

3. Select an AP Load Group from the list on the AP Load Groups Summary page.

4. Click the Edit icon. The AP Load Groups Details page displays. You can change the APs/radios included in the AP Load Group as well as the Band Preferences and Load Control settings for radio balancing Load Groups.

5. Click **OK** to save the changes.

Deleting an AP Load Group

To delete an AP Load Group configuration:

1. Click the Configured Objects tab.

2. In left-hand pane, click AP Load Groups. The AP Load Groups Summary page displays.

3. Select an AP Load Group from the list on the AP Load Groups Summary page.

4. Click the Delete icon. Wireless Manager prompts to verify that you want to delete the selected AP Load Group. Click **OK** to continue or **Cancel** to abort the AP Load Group deletion.

You can also delete an AP Load Group from the AP Load Group Details page.

Managing Wireless Manager Templates (Legacy)

Templates are global configurations that provide a simple, centralized view of how the network ought to be configured. You can create a new template, or clone an existing configuration and modify it to create a new template.

A template takes effect after you create a task to deploy it.

This section includes the following topics:

- [About Templates in Extreme Management Center (Legacy)](#)
- [About Globals Templates in Extreme Management Center (Legacy)](#)
- [About Virtual Network Service (VNS) Templates in Extreme Management Center (Legacy)](#)
- [About WLAN Service Templates in Extreme Management Center (Legacy)](#)
- [About Role Templates in Extreme Management Center (Legacy)](#)
- [About Rate Profiles in Extreme Management Center (Legacy)](#)
- [About AP Profiles in Extreme Management Center (Legacy)](#)
- [About Classes of Service Templates in Extreme Management Center (Legacy)](#)

About Templates in Extreme Management Center (Legacy)

Templates enable you to create one configuration and either store that configuration for later use or deploy it to one or more targets simultaneously. Although you can apply the same template to multiple targets, some templates are more useful with customizations that you can apply when you deploy the template. For example, a VNS template that makes use of a particular VLAN would be much less useful if it forced the administrator to use the same physical port on each target Wireless Controller as the point of attachment to the VLAN. Similarly, you must assign a different subnet range to a routed topology when you deploy a template to different Wireless Controllers. Most templates permit you to customize some settings for each Wireless Controller to which the template is deployed. You can customize some template settings for each Wireless Controller when you deploy the template.

Some types of templates, such as an AP profile template, do not need any per-Wireless Controller customizations. In this case, you can clone an existing template or configuration, make modifications, and save it as a new template.

The template, with its per-Wireless Controller customizations, provides a single point in the UI where you can see how a VNS should be deployed across your Wireless Controllers.

This Help topic includes the following information:

- Template Versions
- Resolving Template Conflicts
- Resolving Duplicate Templates

Template Versions

- Compatibility Versions - In past releases, different versions of Policy and Topology templates were only compatible with specific versions of Wireless Controllers. Consequently, to help avoid conflicting versions of templates and to clarify why certain deployment targets were not available for selection, a Compatibility parameter was added to each template's general properties page. In this release however, all templates are deployable to 8.01 or later Wireless Controllers, within the following

guidelines:

- When migrating from an earlier release of Wireless Manager any V7.31/7.41-Advanced Mode Compatible Policy templates as well as V7.31 - Compatible Topology templates are automatically upgraded to V8.01+ Compatible templates. These templates will appear directly under the Legacy folder in their corresponding sections in the Navigation Tree.

- After the legacy template migration period has expired, any legacy templates (Roles, CoS and Rate Profiles) remaining cannot be deployed. Use Policy Manager to configure these entities on the controller. See Legacy Template Notification.

■ Edit versions — Wireless Manager does not keep historical copies of templates. The edit version is represented by a version number that increments each time you successfully save a template. The edit version number is used primarily to annotate logs pertaining to templates, so that when looking at a template's historical logs, you can determine whether:

- The template is deployed multiple times.

- The same template was deployed (the same edit-version was deployed each time) or different versions of the template were deployed (different edit-version numbers).

Resolving Template Conflicts

After template deployment, Wireless Manager audits the Wireless Controller configurations to ensure that the Wireless Controller configurations do not deviate from the deployed template. When it encounters discrepancies between what ought to be deployed (the template) and what actually is deployed (the Wireless Controller or AP configuration), the Wireless Manager audit feature logs an error.

To address any discrepancies, you can manually launch the Conflict Resolution wizard. Otherwise, when you log in next, Wireless Manager automatically launches the wizard. Using the wizard, you can choose to address and resolve any deviations, or to accept them.

To launch the Conflict Resolution wizard:

1. From the Wireless Manager top banner, click on the Resolve Audit Conflicts button ⬤.

2. For each template that does not match the actual target configuration, select how you would like to resolve the conflict. After the conflict is resolved, the deployment wizards will launch for those templates that require deployment.

3. In the Filter By Type field, you can filter the list of templates which have conflicts to display only those of a particular template type.

4. In the Action field, select one of the following:

   - Do Nothing – Select this option to stop being reminded of the discrepancy between the configuration in Wireless Manager and on the Wireless Controllers.

   - Remind me later – Select to postpone resolving any conflicts.

   - Remove from targets – Select to resolve the conflict by removing from the scope of the template those targets that have conflicting configurations. This will not cause changes to either the Wireless Manager template, or the Wireless Controller's or AP's configuration.

   - Use changed settings – Select to resolve the conflict by cloning the configuration of one of the conflicting targets and deploying it to all of the template's targets.

   - Redeploy and overwrite – Select to resolve the conflict by redeploying the template as it is defined on Wireless Manager to all of the targets. When you redeploy a template to all targets, the template overwrites the conflicting settings on the conflicting targets.

5. Click **Finish**.

6. A message displays whether or not the selected action was successful. A status bar shows the percentage of completion.

Resolving Duplicate Templates

In previous releases of Wireless Manager, selecting the clone and retrieve features did not properly merge entities resulting in duplicate versions of the same template. Now using the Duplicate Resolution wizard, you can have Wireless Manager automatically detect and merge duplicate templates.

To launch the Duplicate Resolution wizard:

1. From the Wireless Manager top banner, click on the Resolve Duplicates button .

2. In the Filter By Type field, you can filter the list of templates which have duplicates to display only those of a particular template type.

3. In the Selection field, select one of the following:

   - Resolve Automatically – Select this option to have Wireless Manager resolve the duplicate template.

   - Select a template – Select a template from a list of existing templates.

4. Click **Finish**.

Editing Templates in Extreme Management Center (Legacy)

You can edit the following Wireless Manager template types at any time: Globals, Virtual Networks (VNS), WLAN Services, and Access Points. Changes will not take effect until you create a task to deploy the modified template.

NOTE: Wireless Manager no longer supports the configuration or editing of Role, Rate Profiles, and Classes of Service templates.

To edit a template:

1. Click the Templates tab.

2. In the left pane, select the type of template you want to edit. The Summary page displays.

3. Select a template in the Summary page and either click the edit icon at the top of the page or right-click on the template name and select Edit from the drop-down menu. You can also expand the template folder in the left pane and select a template to edit.

4. The Template Configuration tabs display with the [Template Properties Tab](#) active. Move between the tabs and change the settings as desired.

5. Click the **Save** button to save the changes.

Related Information

- [About Templates](#)
- [Deleting Templates](#)

Deleting Templates in Extreme Management Center (Legacy)

You can delete any template (except for Roles, Rate Profiles, and Classes of Service) in Wireless Manager using the Delete wizard.

1. Click the Templates tab.

2. Navigate to a Summary page for the configuration you want to delete.

3. Either click the delete icon at the top of the page or right-click on the template name and select Delete from the drop-down menu. The Delete wizard launches.

4. **Select delete options.** The Delete wizard offers options for cleaning up tasks that were created from the template. In addition, it may offer the option of undeploying the template from any of the template's targets. From the options listed, select the deletion and undeployment tasks you want to perform. Then, click **Next** to continue.

5. **Deselect controller for removal (optional).** The Delete wizard offers options for cleaning up tasks that were created from the template. In addition some wizards offer the option of undeploying the template from any of the template's targets.

6. **Select Target to Delete.** Select a target from which you want to undeploy a template. Click **Next**.

7. **Execute Task.** The window displays a status bar that shows the task as it completes. After the task is complete, the system identifies whether the action succeeded or failed.

Related Information

- [About Templates](#)
- [Editing Templates](#)

Extreme Management Center Template Properties Tab

This topic describes the fields available in the Template Properties tab in Wireless Manager. A sample Globals Template Properties tab is shown below.
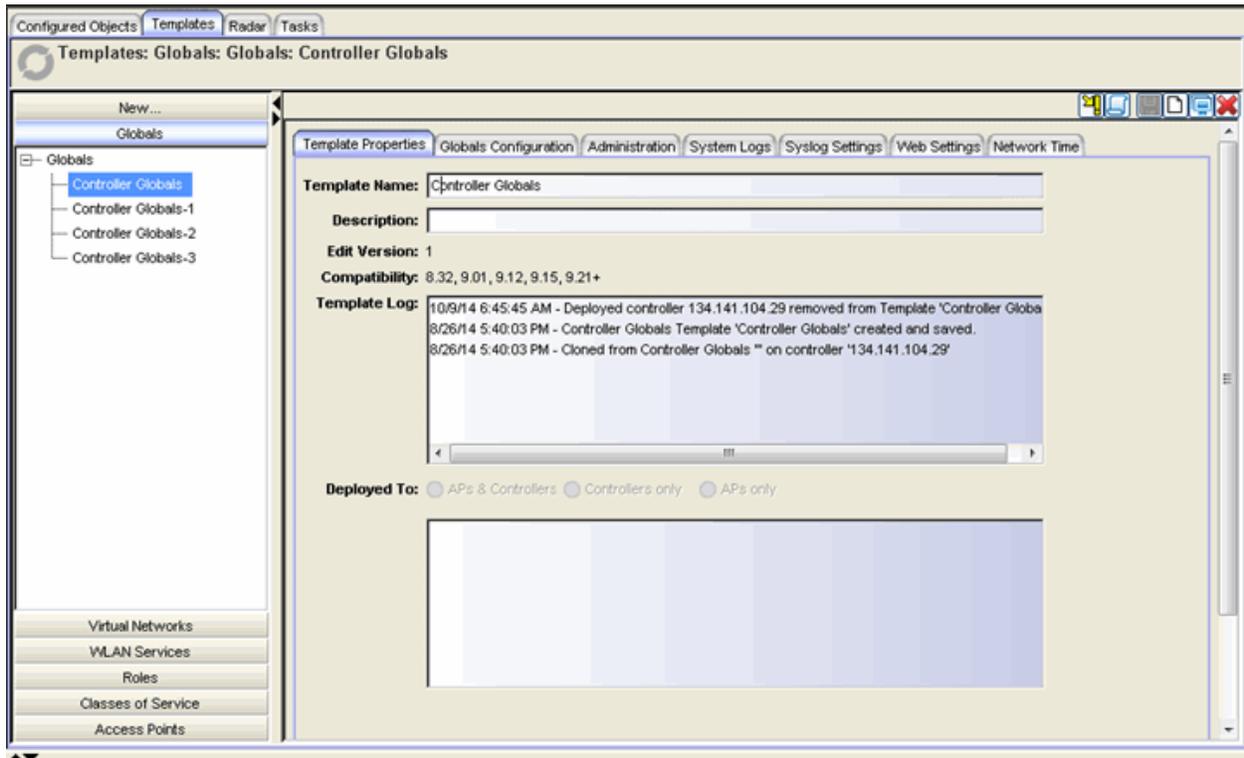
Template Name

Enter a name for this template.

Description

Enter text to describe the purpose of this template (optional).

Edit Version

Increments each time this template is edited.

Compatibility

Displays the versions of the Wireless Controller software that are compatible with this template.

Template Log

The template log lists significant events in the life of the template, such as when it was created, when it was changed, and when it was deployed.

Deployed to
Lists the Wireless Controllers, APs, AP Groups, and AP Load Groups (as applicable for the template type) to which the template is deployed.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Related Information

- [About Templates](#)
- [Deleting Templates](#)
- [Editing Templates](#)

Viewing Detailed Template Information in Extreme Management Center (Legacy)

You can view detailed information about a particular template using the template configuration tabs in Wireless Manager. Using the [toolbar](#) in the tabs, you can also perform the following tasks:

- Deploy or undeploy the template.
- Clone or delete an existing template.
- Edit the template configuration.
- Export a template to the CLI.
- Create a new template definition.

To view detailed information about a template:

1. Click the Templates tab.
2. Expand the template folder in the left pane and select the template you want to view.
3. The Template Configuration tabs display with the [Template Properties tab](#) active.

Related Information

- [About Templates](#)
- [About Radar](#)

About Globals Templates in Extreme Management Center (Legacy)

A Globals template is a general template for configuring global settings on a wireless controller. The settings configured using a Globals template are grouped into the following categories which can be independently configured:

- Administration - Includes Jumbo Frame Support, Synchronize System Configuration (only applicable for availability pairs)
- System Logs - System Log Level, Report station events, Send/forward station sessions
- Syslog Settings - Syslog, Facilities (Application Logs, Service Logs, Audit Logs, Station Logs)
- Web Settings - Web Management Settings
- Network Time - Time Zone Settings, System Time, NTP
- Location Settings - Environment Settings, Location Targets, Location Batch Reporting
- Authentication Settings - RADIUS Servers
- Wireless QoS Settings - Configure Admission Control Thresholds and flexible client access.
- Topology Groups Settings - Algorithms for selecting a member topology from a topology group.

This Help topic includes the following information:

- Creating a Globals Template
  - Manually Creating a Globals Template
  - Cloning Globals
- Viewing Summary Information About All Globals Templates

Creating a Globals Template

You can create a Globals template either manually, or by cloning it from deployed Globals or an existing template.

Manually Creating a Globals Template

To manually create a Globals template:

1. Click the **Templates** tab.

2. In the left pane, click New, expand the New folder and click Add Globals. The Globals Template Configuration page displays with the **Template Properties** tab active.
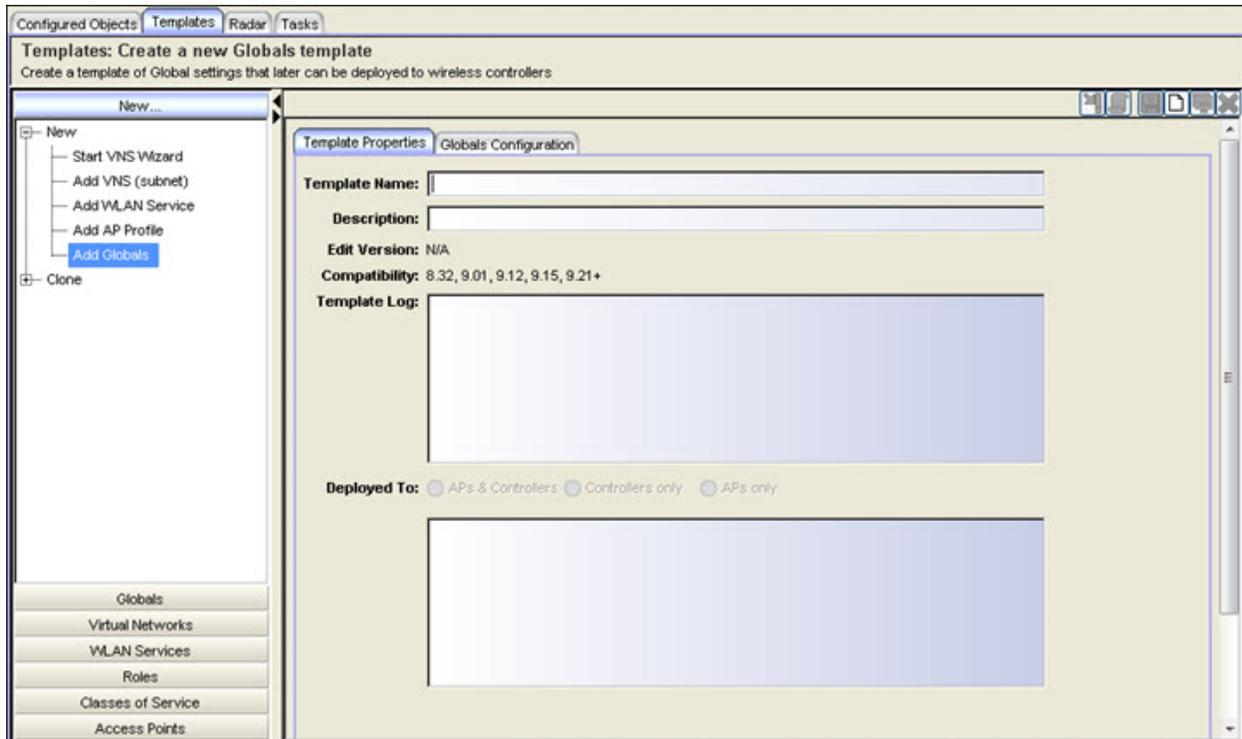
3. Enter a name for the new template. Enter a template description, if desired. For more information about the fields on this tab, see the [Template Properties Tab](#) Help topic.

4. Click on the **Globals Configuration** tab. Select the categories you want to configure. For each selection, a corresponding tab appears. Each of the different tabs are described below.

Administration Tab
Jumbo Frame Support
This feature can be enabled on v9.01 or later controllers. It is supported on the following hardware platforms:

Wireless Controllers:

- Supported: C35, C4110, C5110 and C5210
- Not supported: C25, WLC711 and V2110

Access Points:

- Supported: 37xx APs (except 3705) and 38xx APs
- Not supported: AP26xx, AP36xx, and AP3705

Enabling this feature affects the maximum L3 MTU size for APs and Topologies

Topology Interface L3 MTU:

- For routed topologies: 1436 / 1736 (with Jumbo Frames)
- For BAC topologies: 1500 / 1800 (with Jumbo Frames)
- For Admin / Physical topologies (not supported by Wireless Manager)

AP Tunnel MTU

- For 37xx & 38xx AP profiles the valid range has increased to [600-1800] bytes.
    - If MTU > 1500, Ethernet speed setting MUST be Auto (default) / 1 Gbps (not 10/100 Mbps).
    - If EWC / AP doesn't support jumbo frames, or it is disabled:

      Template Value: x < 1500, 1500 <= x <=1800

      Deployed Value: x < 1500 (no change), x=1500
    - If EWC supports jumbo frames AND AP supports jumbo frames AND it is enabled:

      Template Value: x <=1800

      Deployed Value: x<=1800 (no change)

      In other words, whatever is specified in the template is what gets deployed.

Synchronize System Configuration
Select this checkbox to push the configured VNS definitions from the primary controller to its availability partner.

- WDS, Mesh and 3rd Party AP VNS definitions are not synchronized.

- Synchronizing VNS definitions deletes and replaces any existing VNS definitions on the peer controller.

- All VNS parts are synchronized (VNS, WLANs, Roles, Topologies, CoS)

A Globals Template is always deployed to all target controllers regardless of their paired status and whether or not "Synchronize System Configuration" is enabled. For other types of templates:

- If this setting is enabled, Wireless Manager will only deploy to one of the controllers in an availability pair and leave it to that controller to sync with its peer; the audit process detects any discrepancies.

- If this setting is not enabled, Wireless Manager will deploy to each controller in an availability pair.

System Logs Tab

System Log Level
   Wireless Controller & AP Log Levels: Critical, Major, Minor, and Information.

   - Critical, Major and Minor level logs are considered to be alarm conditions.

   - Information level logs are considered to represent normal operation.

Report station events on controller
   Click to collect and display station session events on the controller's Station Events log.

Send station session to NetSight
   Click to forward station session events to NetSight for monitoring.

Forward station session events as traps
   Click to forward station events as SNMP traps.

Syslog Settings Tab

Syslog
   Enable the Syslog function for up to three syslog servers.The default syslog port (514) cannot be changed. The following settings apply to all configured servers:

- Include all Service Messages:

  - Disabled: Only component messages (logs and traces) are relayed.

  - Enabled: Logs, traces and DHCP messages are relayed.

- Include Audit Messages: relays audit messages.

- Include Station Event Messages: relays station session event messages.

Facilities
Facilities – set level (Local0, Local1, Local3, Local4, Local5, Local6) to be sent to syslog server for:

- Application Logs

- Service Logs (only enabled if Include all Service Messages is selected)

- Audit Logs (only enabled if Include Audit Messages is selected)

- Station Logs (only enabled if Include Station Event Messages is selected)

Web Settings Tab
Web Management Settings
These fields can be entered as hour:minutes, or just minutes. Valid range: 1 minute to 168 hours (or 7 days).

- Web Session Timeout: The length of time that a web session can remain inactive before it times out.

- GuestPortal Manager Web Session Timeout: Same as Web Session Timeout but applies to users of group GuestPortal Manager.

Show WLAN names on the Wireless AP SSID list
Select to allow the names of the WLAN services to appear in the SSID list for Wireless APs.

Network Time Tab
Time Zone Settings

- Continent or Ocean: Large-scale geographic region.

- Country: Contents of drop down change based on the "Continent or Ocean" selected.

- Time Zone Region: Lists those time zone regions appropriate for the selected country.

System Time
Select Configure System Time to set the system time directly.

- Use Deployment Time: Can be scheduled in the future. Converts the server's time into the Wireless Controller's target time zone.

- Set Time: Only makes sense for immediate execution. Entered as mm-dd-yyyy hh:mm. It is assumed to be with respect to the Wireless Controller's target time zone.

NTP

Select Enable to configure NTP. If the Wireless Controller cannot connect to Time Server 1, it will attempt to connect to any additional servers specified. The Time Server fields support IP addresses (IPv4 / IPv6) or FQDNs.

If no Time Servers are specified, "Run local NTP Server" must be selected.

Location Settings Tab

Location Engine Settings

Select **Enable** to configure Location Engine Settings. The Location Engine Settings section of the window allows you to configure the environment in which the AP is functioning to provide greater accuracy. Additionally, within the Location Targets section of the window, you can locate active sessions of users connected to the AP and track users as they move between areas in maps you configure through the use of triangulation, by selecting the **Locate Active Sessions** and **Track Area Change** checkboxes, respectively. Areas are configured in maps on the **Network** tab in Extreme Management Center. For additional information about configuring areas in maps, see [Configure Area window](#).

Environmental Settings

- Default AP Height (cm): Enter the height of the wall-mounted AP in centimeters.

- 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:
  - 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.

Location Batch Reporting
Select Enable to configure Location Batch Reporting.

- 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.

- Post all location destinations to the following URLs: List of destination URLs.

Authentication Settings Tab

RADIUS Servers
Select to enable Strict Mode. When Strict Mode is enabled, all WLANs on a controller that require RADIUS Servers will use the top three global RADIUS servers configured for 'Auth' and 'Acct' accordingly. If the prioritization of these global RADIUS servers changes so will those referenced by the WLANs.

MAC Address Format: Configure the global MAC address format to use with the RADIUS Servers from the drop-down.

Advanced button
Click the **Include the Service-Type attribute in Client Access Request messages** checkbox to include Service-Type attribute in Client Access Request messages. Default is disabled.

If the **Include the Service-Type attribute in Client Access Request messages** checkbox is selected, the **Set Service-Type to Login** checkbox is available. Click the **Set Service-Type to Login** checkbox to set the Service-Type attribute to Login. When this option is not selected, the Service-Type attribute in the Attribute-Request message is set to Framed. Default is disabled.

NOTE: If the Wireless Controller is using the RADIUS login, this option is not available.

Enter the number of seconds to set the Delay for Client Message for Topology Change. This setting specifies how long a notice web page displays if a topology change occurs during authentication as a result of a

role change. The notice web page indicates that authentication was successful and that the user must restart the browser to gain access to the network.

For Authentication, select one of the following options:

- Send requests to Primary whenever it is up (Primary-Backup). Gives the administrator the ability to configure whether the primary server should resume client authentication when it has recovered. Currently it is only supported for RADIUS authentication and not accounting.

- Send request to one server until it fails (Round-Robin). When multiple RADIUS servers are specified for client authentication, one server is used as the primary server, but if that server fails then authentication is transferred to the next server, and so on. Only the last working RADIUS server remains active in authenticating clients.

Select the **RADIUS Accounting** checkbox to activate RADIUS accounting for WLAN Services for which RADIUS accounting is configured. Default is enabled.

NOTE: Disabling the Radius Accounting checkbox overrides the RADIUS accounting settings of individual WLAN services. Enabling RADIUS accounting activates RADIUS accounting only in WLAN services specifically configured to perform it.

Select **Defer sending the accounting start request until the client's IP address is known** to configure the start of RADIUS accounting to occur after the client receives an IP address.

Wireless QoS Tab

Admission Control Thresholds

Select the percentage of bandwidth for the following streams:

- **Max Voice (VO) BW for roaming streams** - Set the maximum percentage of bandwidth for roaming voice streams as a percentage of the total bandwidth.

- **Max Voice (VO) BW for new streams** - Set the maximum percentage of bandwidth for new voice streams as a percentage of the total bandwidth.

- **Max Video (VI) BW for roaming streams** - Set the maximum percentage of bandwidth for roaming video streams as a percentage of the total bandwidth.

- **Max Video (VI) BW for new streams** - Set the maximum percentage of bandwidth for new video streams as a percentage of the total bandwidth.

- **Max Best Effort (BE) BW for roaming streams** - Set the maximum best effort bandwidth for roaming streams as a percentage of the total bandwidth.

- **Max Best Effort (BE) BW for new streams** - Set the maximum best effort bandwidth for new streams as a percentage of the total bandwidth.

- **Max Background (BK) BW for roaming streams** - Set the maximum background bandwidth for roaming streams as a percentage of the total bandwidth.

- **Max Background (BK) BW for new streams** - Set the maximum background bandwidth for new streams as a percentage of the total bandwidth.

Flexible Client Access

Select the airtime or packet fairness for WLAN participants. Airtime fairness gives WLAN participants the same time access and a client's throughput is proportional to their PHY rate. Packet fairness gives WLAN participants the same opportunity to send packets and all clients will show the same throughput, regardless of PHY rate.

NOTE: Flexible Client Access may not work if Global Admission Controls for Voice, Video, Best Effort, or Background are enabled.

Topology Groups Settings Tab

Topology Group Selection Algorithm

Select the algorithm used to select a topology from a topology group. Options include:

- MAC Based - The topology is selected by converting the MAC address to a number, dividing that number by the number of topologies in the group, and using the topology that corresponds to the resulting number.

- Round Robin - The topologies are listed in order and each topology is selected in turn.

- Random Selected - The topologies are randomly selected uniformly.

- Least Used - The topology to which the least number of stations assigned is selected at the moment of assignment is selected.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Cloning Globals

To create a Globals template by cloning an existing template or configuration:

1. Click the **Templates** tab.

2. In the left pane, click New, expand the Clone folder and click Clone Globals. The Clone Globals wizard launches.

3. On the Cloning Source dialog, enter a name for the new template in the New Template Name field.

4. Select one of the following:

   - Base template on a deployed Globals – This option lets you create a template by copying those global settings, which Wireless Manager allows you to configure, from a Wireless Controller.

   - Base template on an existing Globals – This option lets you create a template by copying the settings of another already existing Globals template.

5. The window that lists the selected items becomes active. Click the **View Selected** button to view detailed information about the cloning source.

6. Click **Next**.

7. The Cloning Summary page displays the Globals configuration that you selected. Click **Finish** to clone the Globals template or **Cancel** to discard it.

Viewing Summary Information About All Globals Templates

You can view summary information about Globals currently defined in Wireless Manager from the Globals Summary page. From this page, you can also perform the following tasks:

- Deploy or undeploy the template.

- Edit, clone, or delete an existing Global definition.

- Export a Global configuration to the CLI.

- Create new Global definition.

To view summary information about configured Global:

1. Click the **Templates** tab.

2. In left-hand pane, click Globals. The Globals Summary page displays.
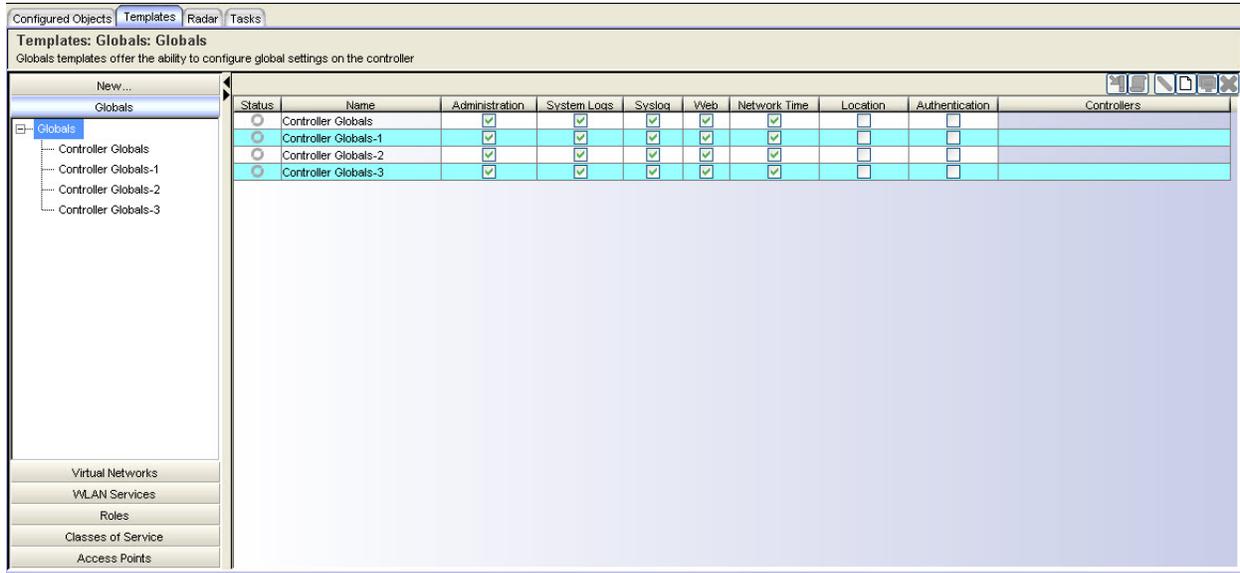
The following list describes the information available on the Globals page.

Status

Status of this Global. Options include:

⊙ Deployed, ⊙ Not Deployed, 🚫 Deployed but not synchronized to the network,

🚫 Deployed but some templates not synchronized.

Name

Name assigned to the Global.

Administration

Indicates if Administration settings are deployed to the Wireless Controller. Options are: enabled or disabled.

System Logs

Indicates if System Logs settings are deployed to the Wireless Controller. Options are: enabled or disabled.

Syslog

Indicates if Syslog settings are deployed to the Wireless Controller. Options are: enabled or disabled.

Web

Indicates if web settings are deployed to the Wireless Controller. Options are: enabled or disabled.

Network Time

Indicates if Network Time settings are deployed to the Wireless Controller. Options are: enabled or disabled.

Controllers

Wireless Controller to which this Globals template has been deployed.

Location

Indicates if this Globals template defines Location related settings (Engine / Batch Reporting) to be deployed to target Wireless Controllers.

Authentication

Indicates if this Globals template defines Authentication related settings to be deployed to target Wireless Controllers.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Related Information

- [Deleting Templates](#)
- [Editing Templates](#)
- [Viewing Detailed Template Information](#)

About Virtual Network Service (VNS) Templates in Extreme Management Center (Legacy)

A Virtual Network Service (VNS) is a binding of several reusable components that together provide a versatile method of mapping wireless networks to the topology of an existing wired network. It is composed of a WLAN service with one or more roles that control the wireless station's access to the wired network.

If you are not using the VNS wizard to create a VNS template, you should already have configured templates for the following elements:

- Topologies - A topology is a combination of Layer 2 and if applicable, Layer 3 networking attributes.

- Class of Services - A CoS refers to the set of attributes that define the importance of a frame relative to others on the network. It is a configuration entity containing QoS Marking (802.1p and ToS/DSCP), Inbound/Outbound Rate Limiting and Transmit Queue Assignments.

- Roles - A role defines the default access control, egress VLANs, filter rules, and Class of Service to be applied to the traffic of a station.

- WLAN Services - A WLAN Service defines and the radio attributes, privacy and authentication settings, and QoS attributes of the VNS.

This Help topic includes the following information:

- [Creating a VNS Template](#)
- [Viewing Summary Information About All VNSs](#)

Creating a VNS Template

When using the VNS wizard, you can create a VNS for many different purposes, including:

- Voice - Voice-specific VNS that can support various wireless telephones, including WL2, SpectraLink, Polycom Spectralink 8000, ASCOM - i62, Vocera - Smartphone, Vocera - B2000, Vocera - B1000, Mobile Connect - Nokia.

- Data - Data-specific VNS, that can be configured to use either SSID or AAA authentication.

- Captive Portal/NAC-Compatible Captive Portal-based VNS - 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.

- NAC Compatible EAP-based VNS - NAC EAP-compatible VNS. The ExtremeWireless Wireless Controller integrates with an EOS NAC Controller to provide authentication, assessment, remediation and access control for mobile users.

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

There are three ways that you can create a VNS template. For instructions, see:

- [Creating a VNS Configuration Using the VNS Wizard](#)
- [Manually Creating a New VNS Configuration](#)
- [Cloning an Existing VNS](#)

The VNS configuration does not take effect until you create a task to deploy it.

Creating a VNS Configuration Using the VNS Wizard

The VNS wizard steps you through the configuration and prompts you for a minimum amount of configuration information. After the VNS wizard completes the VNS template creation process, you can then continue to configure or revise the VNS template configuration to suit your network needs.

Using the VNS wizard you can create VNS that are deployable to Policy Manager (PM) managed Wireless Controllers and non-PM managed Wireless Controllers. However, after the legacy template migration period has expired, you can only create VNS deployable to PM managed EWCs (see [Legacy Template Migration Notice](#)). A controller is considered managed by Policy Manager if it is assigned to a Policy Manager domain. By default, the VNS wizard creates a VNS which can be deployed to PM managed Wireless Controllers. If you want to create a 'Legacy' VNS that can be deployed to non-PM managed Wireless Controllers, click the Legacy checkbox on the first page of the wizard.

To launch the VNS Wizard:

1. Click the Templates tab.

2. In left-hand pane, click New, expand New and click Start VNS Wizard. The VNS Template Configuration wizard launches.

3. Enter a unique name for the VNS.

4. Select the category of VNS you want to create. Options include:

    - Voice

    - Data

    - Captive Portal

    - NAC-compatible Captive Portal-based VNS

    - NAC-compatible EAP-based VNS

5. Click Legacy to create a VNS that can only be deployed to non-PM managed Wireless Controllers.

6. Click **Next**. The Set Basic Settings Window displays.

Set Basic Settings Window

NOTE: The contents of the basic settings window will vary based on the type of VNS that you are creating.

7. Click Enabled to enable this VNS by default.

8. In the SSID field, enter an SSID. By default, the value you specified in the Name field in the previous window automatically populates this field.

9. In the Type field, select the type of VNS you want to create from the drop-down menu. This field is not present for Data VNS.

10. In the Mode field, select the type of topology. Depending on the category of the VNS and whether or not it is a Legacy VNS, options may include:

    - Routed

    - Bridged Traffic Locally at AP (B@AP)

    - Bridge Traffic Locally at Wireless Controller (B@EWC)

11. Specify a VLAN ID. For a Legacy VNS with a mode of B@AP or B@EWC specify whether it is tagged and if necessary its VLAN ID.

12. For a Voice VNS, enter an IP address for the PBX server/Gateway - SVP/Vocera Server.

13. If available, select Enable Authentication to enable authentication on this VNS.

14. If available, select Enable Filtering to enable filtering for this VNS.

15. Click **Next**.

Define Privacy Settings

16. Select the privacy settings. The privacy settings that you can configure will differ depending on the kind of VNS being created.

Set Authentication

> **NOTE:** Some types of VNS, such as a NAC compatible VNS, do not require input on authentication settings and will skip this window.

17. Select a RADIUS server to be used for authentication from the drop-down menu.

18. If a suitable RADIUS server does not exist, click New to create a new RADIUS server configuration.

> **NOTE:** You can override this selection after you have selected the Wireless Controllers to which to deploy this VNS.

You can optionally choose MAC-based authentication. Additional authentication settings depend on the target Wireless Controller. You can specify these settings when you deploy this template.

Summary

19. Review the summary information. To change any settings, use the **<Prev** button. Click **Finish** to create the VNS template using the settings specified.

After the template is successfully created, you can deploy it by clicking the **Deploy** button in the Creation of VNS Template window.

Manually Creating a New VNS Configuration

To manually create a VNS template:

1. Click the Templates tab.

2. In left-hand pane, click New, expand New and click Add VNS (subnet). The VNS Configuration page displays with the Template Properties tab active.
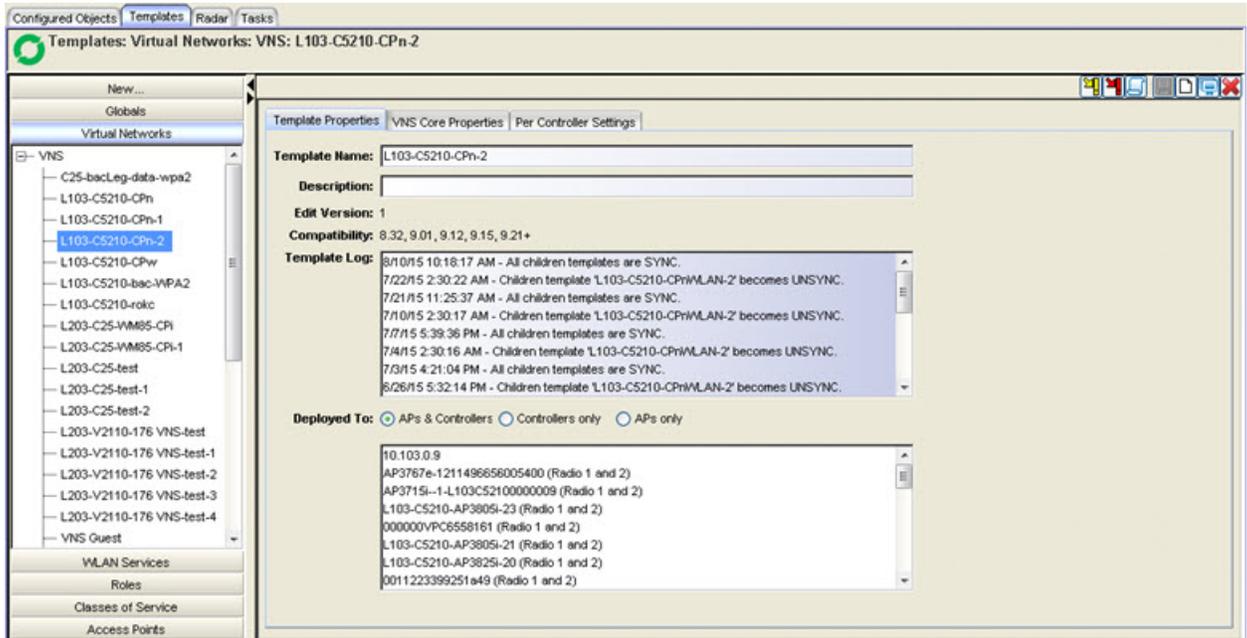
3. Enter a name for the new template. Enter a template description, if desired. For more information about the fields on this tab, see the Template Properties Tab Help topic.

4. Click the VNS Core Properties tab.

5. In the Core area, enter the Name of the VNS.

6. In the WLAN Service area, select the name of the WLAN service from the drop-down menu. If a suitable WLAN service does not exist, you can create one. For more information, go to Creating a WLAN Service Template.

7. In the Default Roles area:

   a. Select a Non-Authenticated role from the drop-down list. A Non-Authenticated role is the role applied by default to a station prior to the station authenticating via 802.1x or captive portal.

   b. Optionally select an Authenticated role from the drop-down list. An Authenticated role is the role applied by default to any station that authenticates successfully and for which no other role has been assigned explicitly.

8. In the Status area, select Enable to enable this VNS when it is deployed.

9. Click the Per Controller Settings tab.

   a. In the Topology Per Controller Settings area, view the Topology settings for both Authenticated and Non-Authenticated Roles.

   b. In the WLAN Service Per Controller Settings, view the RADIUS server
       and Captive Portal settings.

10. Click **Save** to save the VNS.

Cloning an Existing VNS

You can clone an existing VNS template or VNS configuration and modify it to
create a new template or configuration.

To launch the Clone VNS wizard:

1. Click the Templates tab.

2. In left-hand pane, click the New bar, expand Clone and select Clone VNS.
    The Clone VNS wizard launches.

3. On the Select Cloning Source dialog, in the New template name field, enter
    a name for the new VNS.

4. Select one of the following:

    - Base template on a deployed VNS – This options lets you create a
       template by copying the settings of a VNS deployed on a Wireless
       Controller.

    - Base template on an existing VNS – This option lets you create a
       template by copying a template that already exists on the Wireless
       Controller.

5. The window that lists the selected item becomes active. Click the View
    Selected button to view detailed information about the cloning source.

6. Click **Next**.

7. The Cloning Summary page displays the configuration that you selected.
    Click **Finish** to clone the configuration or **Cancel** to discard it.

NOTE: When you create a clone of a template that references other templates, the clone will
continue to reference the same child templates as the original template; it is a shallow
clone. Similarly, when you clone a template based on a deployed entity, if a template
already exists for a child entity it will be reference by the clone, otherwise a new
template is created.

Viewing Summary Information About All VNSs

You can view summary information about VNS templates or configurations
currently defined in Wireless Manager from the VNS Summary page. From this

page, you can also perform the following tasks:

- Deploy or undeploy the template.

- Edit, clone, or delete an existing VNS definition.

- Export a VNS configuration to the CLI.

- Create new VNS definition.

To view information about a configured VNS:

1. Click the Templates tab

2. In left-hand pane, click VNS. The VNS Summary page displays.
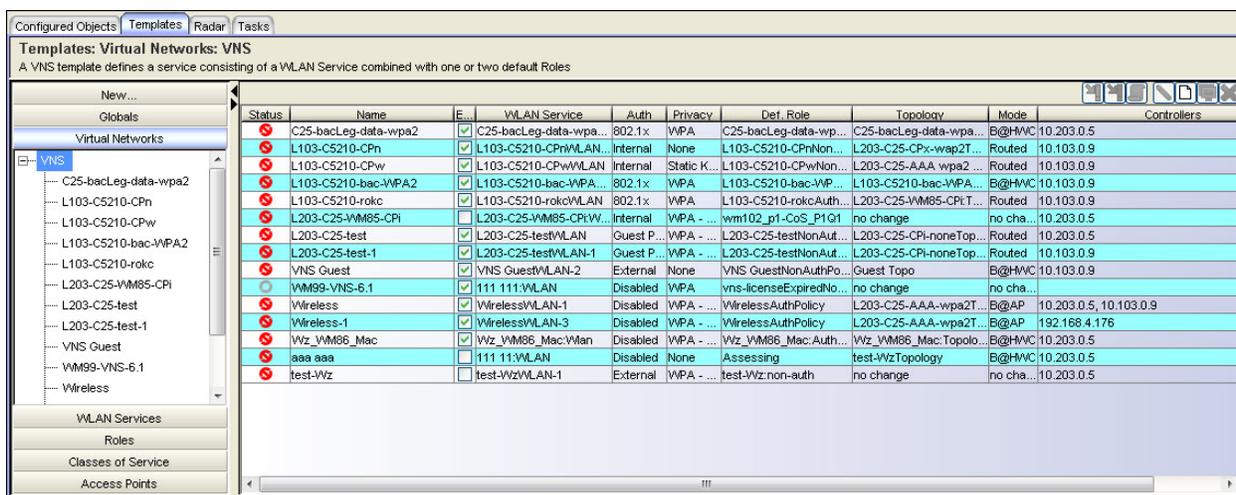
The following list describes the information available on the VNS Summary page.

Status
Status of this VNS. Options include:

🟢 Deployed, ⚪ Not Deployed, 🚫 Deployed but not synchronized to the network,

🚫 Deployed but some child templates are not synchronized,

⚠️ Incomplete - The definition of this template must be completed before it can be deployed.

Name
Name of the VNS. This name can be the same as the VNS template name, or it can be a different name.

Enabled
State of the VNS; the VNS is deployed in an enabled or disabled state.

WLAN Service

The WLAN service used in this VNS.

Auth

The authentication method used by this VNS.

Privacy

The privacy setting for this VNS.

Def. Role

The role used by this VNS.

Topology

The topology used by this VNS.

Mode

The mode of operation of the topology. Values are: Routed, B@AP, or B@EWC used by this VNS.

Controllers

List of Wireless Controllers that use this VNS.

Toolbar Buttons

For a description of common toolbar buttons see <u>Context-Sensitive Toolbar</u>.

Related Information

- <u>Deleting Templates</u>
- <u>Editing Templates</u>
- <u>Viewing Detailed Template Information</u>

About WLAN Service Templates in Extreme Management Center (Legacy)

A WLAN Service represents all the RF, authentication and QoS attributes of a wireless access service offered by the Wireless Controller and its APs. Wireless Manager only supports the configuration of standard and remotable WLAN Services.

Standard - Only APs running ExtremeWireless Wireless software can be part of this WLAN Service. This type of service may be used as a Bridged at Controller, Bridged at 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.

Remotable - Any WLAN service can be made remotable by selecting this property in its Advanced settings dialog. When deploying a remotable WLAN, for each Mobility Zone identified among the selected targets you must choose one Wireless Controller (its home controller) where it will be deployed as remotable; any other selected targets in that Mobility Zone will receive the remote definition of the WLAN. A remote service definition doesn't include any Auth & Acct settings, but should have the same SSID name and privacy settings as its corresponding remotable service.

This Help topic includes the following information:

- Creating a WLAN Service Template
- Viewing Summary Information About All WLAN Services Templates

Creating a WLAN Service Template

You can create a WLAN Service template either manually, or by cloning an existing template or a WLAN Service configuration. When you create a WLAN Service template, you perform the following tasks:

- Define SSID and privacy settings for the wireless link.
- Configure the method of credential authentication for wireless users (None, Internal CP, External CP, GuestPortal, 802.1x[EAP]).
- Configure QoS settings for stations accessing the network through this WLAN Service.

Manually Creating a WLAN Service Template

To manually create a WLAN Service template:

1. Click the Templates tab.

2. In the left pane, expand New and click Add WLAN Service. The WLAN Service Template Configuration page displays with the Template Properties tab active.
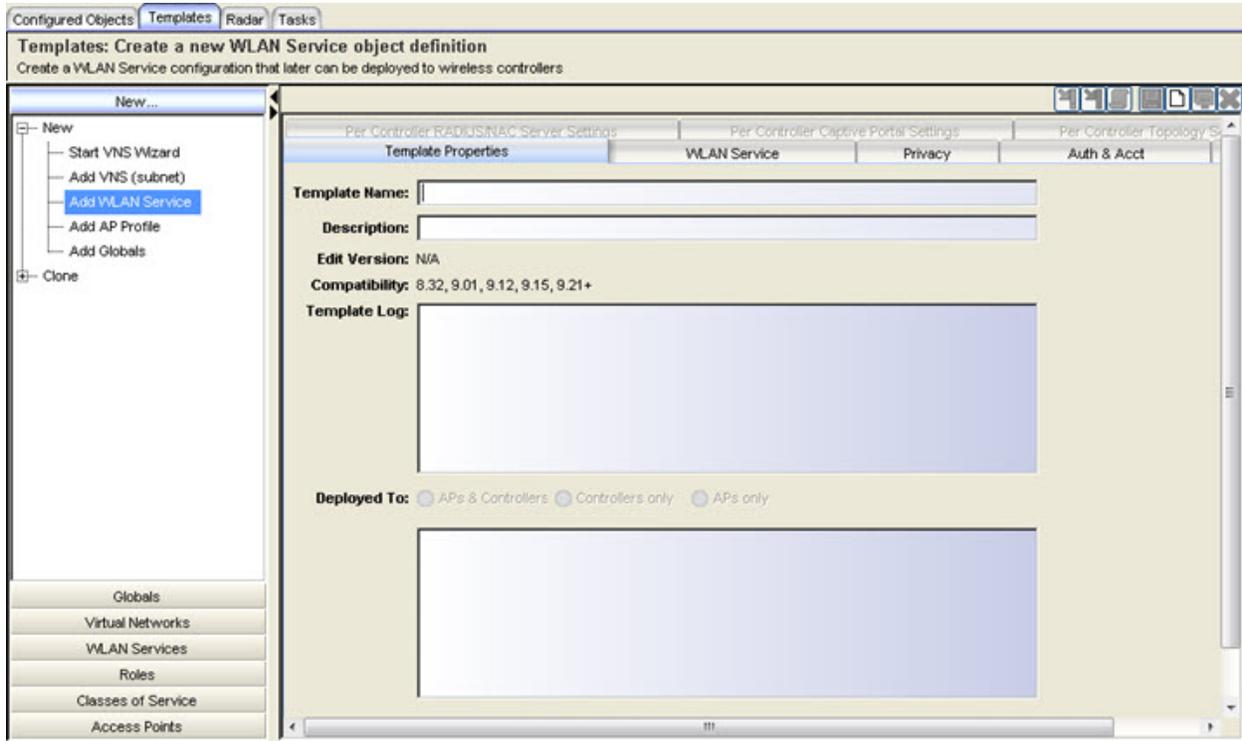
3. Enter a name for the new template. Enter a template description, if desired. For more information about the fields on this tab, see the Template Properties Tab Help topic.

4. Use the other tabs to configure your template. Each of the different tabs are described below.

WLAN Service Tab

Core

Name

Name of this WLAN Service. This name can be the same as the WLAN Service template name, or it can be a different name.

SSID

Service Set Identifier (SSID) is the name of a wireless local area network (WLAN).

NOTE: To prevent the configuration of an unsecure WLAN, a dialog box displays if the SSID exists on a list of hotspot/default SSIDs or if the SSID is on a list of SSIDs for which password cracking tables are available. Click OK to proceed.

Service Type

The service type is always set to Standard.

Default Topology

Name of the default topology used by this WLAN Service. Select a topology from the drop-down menu. The Default Topology setting is optional. 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 role (by default, Bridged at AP Untagged).

NOTE: Wireless Manager imports all VLANs (as topologies) from PM whether or not they are referenced by a specific policy, but only from domains with assigned Wireless Controllers. Any imported VLAN can be configured as the default topology for a WLAN.

Default CoS

Select a defined CoS from the drop-down list, or select the default "No CoS". 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 role.

Status

Select the Enable checkbox to enable WLAN Service.

Advanced Button

Click the **Advanced** button to open a window where you can configure advanced WLAN Service settings. For more information, see <u>Advanced WLAN Service Settings Window</u>.

Privacy Tab
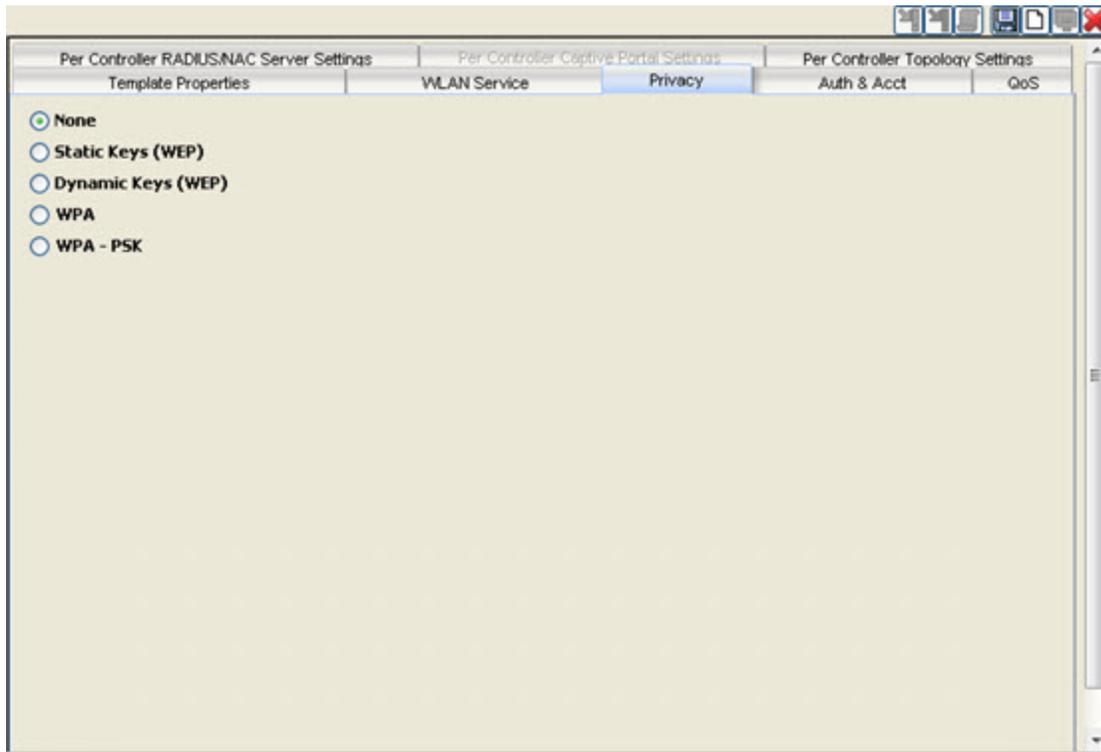
Some privacy settings require compatible authentication settings. For example, WPA requires 802.1x authentication and at least one configured RADIUS server. For more information, refer to the *Extreme Networks Wireless Software User Guide.* Options include:

None, Static Keys (WEP), Dynamic Keys (WEP), WPA, WPA - PSK

> **NOTE:** WPA/WPA-PSK requires a mixed mode setting of WPAv1 and WPAv2 when deploying privacy with 11n APs (for example, AP37xx) to an 8.32+ Wireless Controller. If only WPAv1 is selected in the WLAN template, then when deployed to an 8.32 or later Wireless Controller the resulting WLAN will have both WPAv1 and WPAv2 enabled.

Auth & Acct Tab

The Auth & Acct tab options vary depending on the Authentication Mode selected. The options described below with are available when **Internal** is selected as the Authentication Mode.
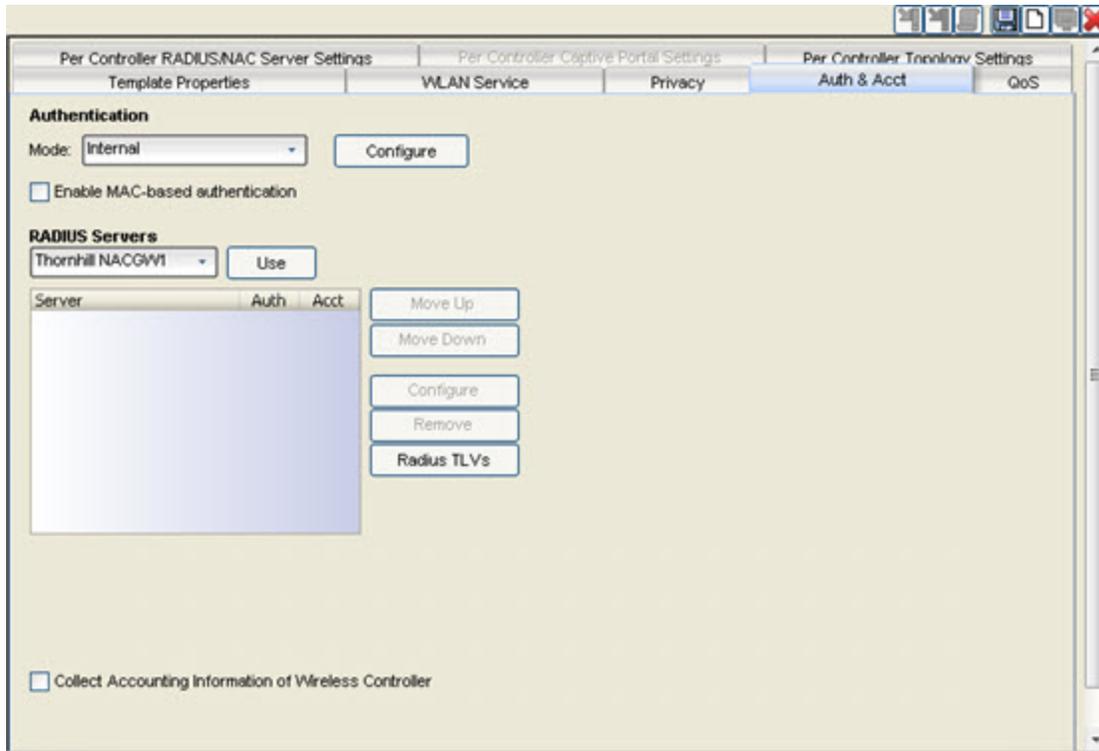
Authentication

Mode
Options include:

- Disabled — to configure a WLAN Service with no authentication
- Internal — to configure Captive Portal
- 802.1x
- External
- Firewall Friendly External
- Guest Portal
- Guest Splash

Click the **Configure** button to open a window where you can configure Authentication Settings that vary depending on the Authentication Mode you have selected. For more information, see Settings Window.

Enable MAC-based authentication
Select the checkbox to enable the RADIUS server to perform MAC-based authorization. Click the **Configure** button to enable the following options:

- **MAC-based authorization**: Select between none, on roam, or on area roam.

- **Automatically Authenticate Authorized Users**: When enabled, 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**: Enable this option to permit 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.

- **RADIUS accounting begins after MAC-based authorization completes**

NOTE: Both the Authentication Mode and the Enable MAC-based authentication 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.

RADIUS Servers

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

Click **Configure** to open the RADIUS Parameters dialog.

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 ExtremeWireless Wireless Controller and the RADIUS server. To proofread your shared secret key, click Unmask. The password is displayed.

Select Fast Failover Events to allow the controller receiving the session to immediately begin sending out interim accounting records. This feature can be enabled for any type of authentication and applies only to controllers in availability with fast failover enabled. Default is disabled.

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

VSAs

Select the appropriate checkboxes to include specific VSA (Vendor Specific Attributes) in the message to the RADIUS server.

Zone Support

Select the checkbox to replace the called station ID with zone.

Optional TLVs

Select the checkbox to enable chargeable user identity. Additionally, this section allows you to configure your system to treat an Access-Accept with no CUI attribute as an Access-Reject.

Operator Name

Specify the name of the user assigned to this RADIUS server by first selecting a namespace ID from the drop-down list. Once a namespace ID is selected (which identifies the format of the name), a text box displays to allow text to be entered. By default it is disabled.

Valid namespace IDs include:

- TADIG ('0' (0x30)),
- REALM ('1' (0x31)),
- E212 ('2' (0x32)),
- ICC ('3' (0x33)).

For more information, see: http://tools.ietf.org/html/rfc5580

The following options described below with are available when **Guest Portal** or **Guest Splash** are selected as the Authentication Mode.
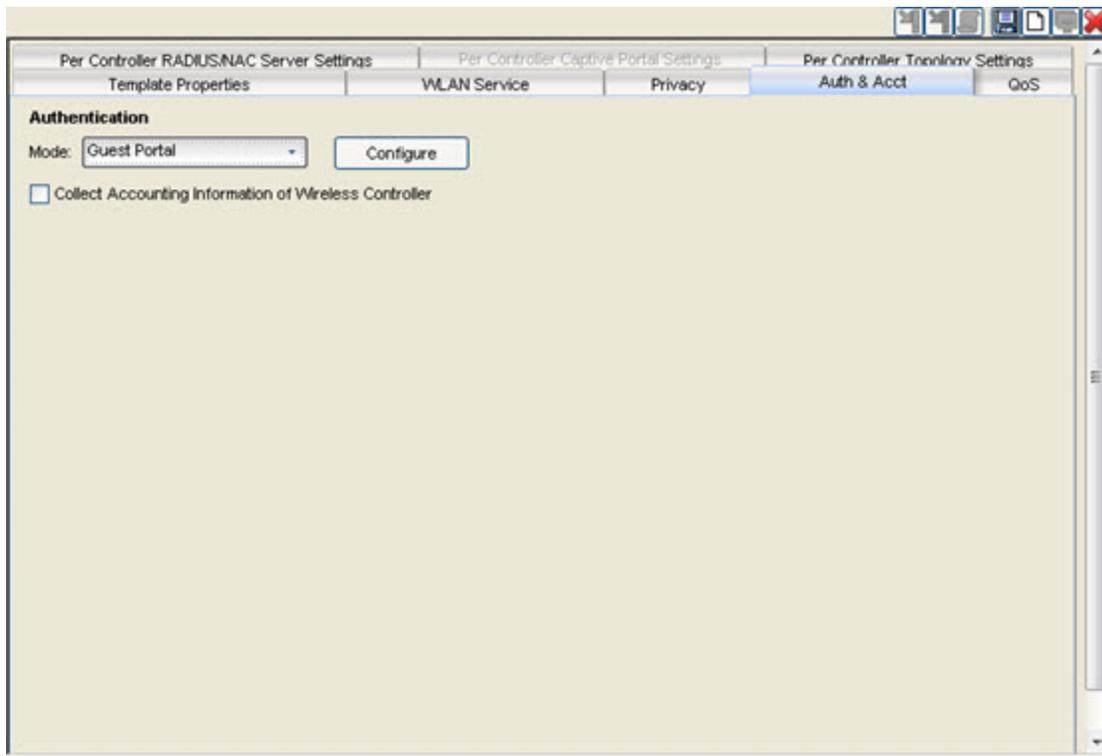
Collect Accounting Information of Wireless Controller

> Select the checkbox to collect information from the Wireless Controller.

Click the **Configure** button to open a window where you can configure Authentication Settings that vary depending on the Authentication Mode you have selected. For more information, see Settings Window.

QoS Tab
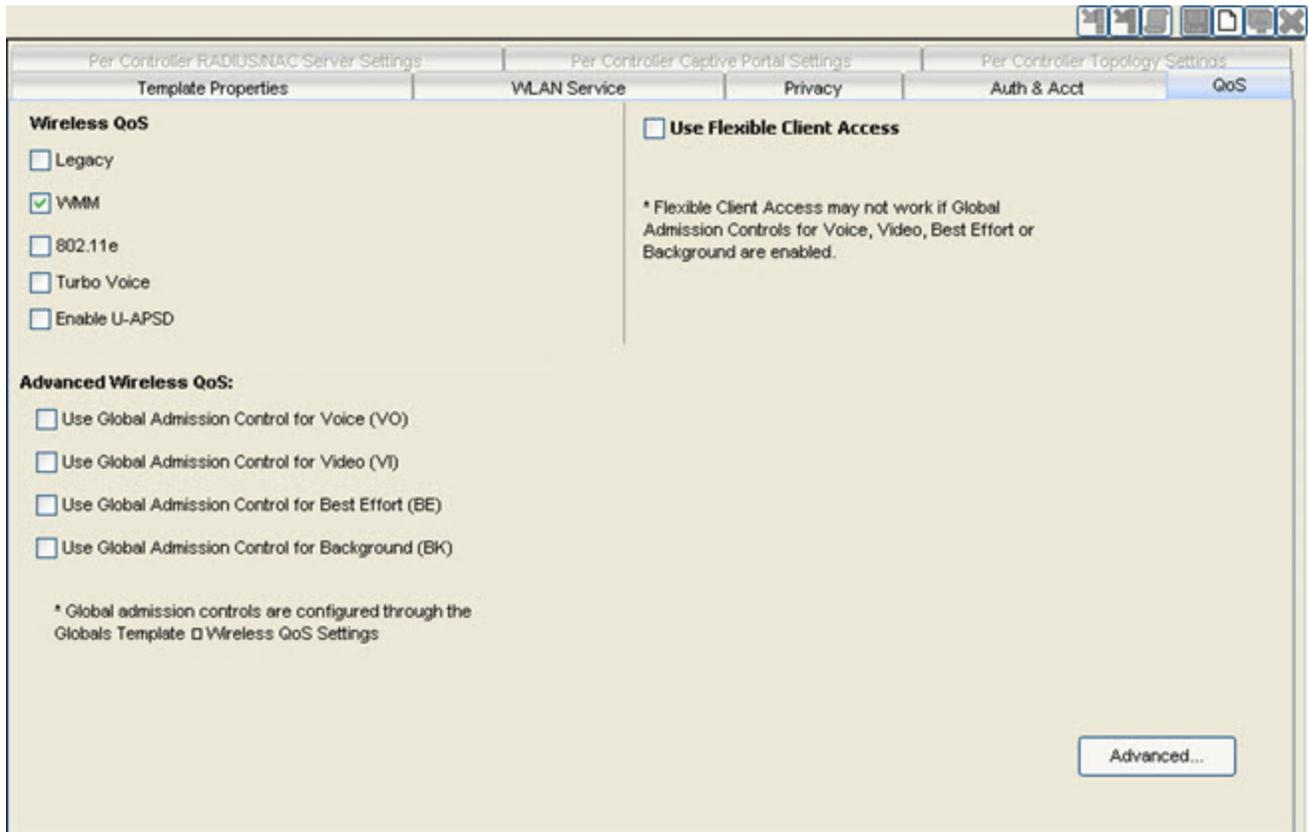
Wireless QoS

Legacy — Select if your service supports legacy devices. AP classifies and prioritizes the out traffic for all clients according to the same rules. Not supported by 38xx APs or controllers running version 9.21 or later. By default it is disabled.

WMM — Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all WMM clients. Note that WMM clients will also classify and prioritize the uplink traffic. WMM is part of the 802.11e standard for QoS. If selected, the Turbo Voice and Enable U-APSD options are displayed.

802.11e — Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic. If selected, the Turbo Voice and the Enable U-APSD options are displayed:

- Turbo Voice — Select to enable all downlink 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 (TVO) 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. Not supported by 38xx APs.

- 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.

Use Flexible Client Access

Click to enable flexible client access.

Advanced Wireless QoS

(VO) — Select to enable Global Admission Control for Voice.

(VI) — Select to enable Global Admission Control for Video.

(BE) — Select to enable Global Admission Control for Best Effort.

(BK) — Select to enable Global Admission Control for Background.

Advanced Button

Click the **Advanced** button to open a window where you can configure advanced QoS settings. For more information, see Advanced QoS Settings Window.

Per Controller RADIUS/NAC Server Settings Tab

Identifies the NAC and RADIUS settings specific to a particular Wireless Controller. This tab is available once a template has been deployed.

Per Controller Captive Portal Settings Tab

Identifies the captive portal settings specific to a particular Wireless Controller. This tab is available once a template has been deployed.

Per Controller Topology Settings Tab

Identifies the topology settings specific to a particular Wireless Controller. This tab is available once a template has been deployed.

Cloning an Existing WLAN Service

To create a WLAN Service template by cloning an existing template or configuration:

1. Click the Templates tab.

2. In the left pane, click New, expand Clone, and click Clone WLAN Service. The Clone WLAN Service wizard launches.

3. On the Cloning Source dialog, in the New template name field, enter a name for the new WLAN Service.

4. Select one of the following:

   - Base template on a deployed WLAN Service – This option lets you create a template by copying the settings of a WLAN Service deployed on a Wireless Controller.

   - Base template on an existing WLAN Service – This option lets you create a template by copying a template that already exists on the Wireless Controller.

5. The window that lists the selected item becomes active. Click the **View Selected** button to view detailed information about the cloning source.

6. Click **Next**.

7. The Cloning Summary page displays the WLAN Service configuration that you selected. Click **Finish** to clone the WLAN Service or **Cancel** to discard it.

Viewing Summary Information About All WLAN Services Templates

You can view summary information about WLAN Services currently defined in Wireless Manager from the WLAN Services Summary page. From this page, you can also perform the following tasks:

- Deploy or undeploy the template.

- Edit, clone, or delete an existing WLAN Service definition.

- Export a WLAN Service configuration to the CLI.

- Create new WLAN Service definition.

To view information about configured WLAN Services:

1. Click the Templates tab.

2. In left-hand pane, click WLAN Services. The WLAN Services Template Summary page displays.

The following list describes the information available on the WLAN Services page.

Status

Status of this WLAN Service. Options include:

⬤ Deployed, ⬤ Not Deployed, ⬤ Deployed but not synchronized to the network,

⬤ Deployed but some templates not synchronized.

Name

Name assigned to the WLAN Service.

Enabled

Whether the WLAN Service created from this template will be deployed in the enabled or disabled state. Options are: enabled or disabled.

Type

Type of WLAN Service.

SSID

Service Set Identifier (SSID) is the name of a wireless local area network (WLAN).

Auth

Authentication mode assigned to this WLAN Service.

Privacy

Privacy settings for this WLAN Service.

Controllers

Wireless Controller to which this WLAN Service has been deployed.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Related Information

- [Deleting Templates](#)
- [Editing Templates](#)
- [Viewing Detailed Template Information](#)

Extreme Management Center Advanced QoS Settings Window (Legacy)

Use this Wireless Manager window to configure advanced WLAN Service QoS settings. To access this window, click the **Advanced** button in the [QoS Tab](#).
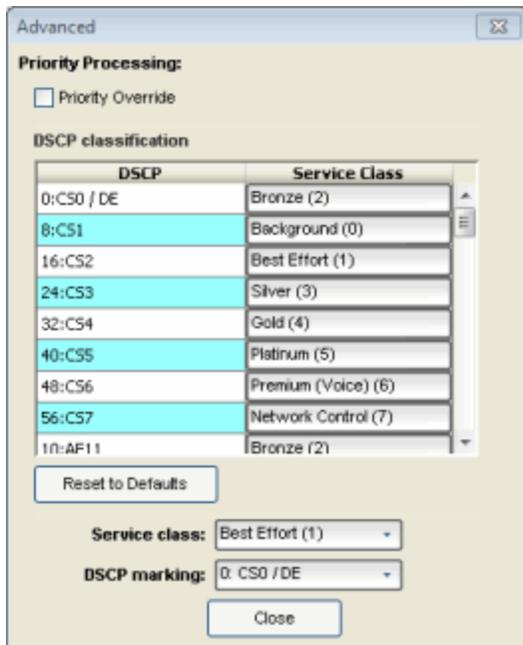
Priority Processing
    Click Priority Override to force a service class and DSCP marking. When enabled, the configured service class forces queue selection in the downlink direction, the 802.11P user priority for the VLAN tagged Ethernet packets and the user priority for the wireless QoS packets (WMM or 802.11e), according to the mapping between service class and user priority.

Service Class
    From the drop-down list, click the appropriate priority level:

- Network control (7) - highest priority level
- Premium (Voice) (6)
- Platinum (5)
- Gold (4)
- Silver (3)
- Bronze (2)

- Best Effort (1)

- Background (0) - lowest priority level

DSCP marking

From the drop-down list, click the DSCP value used to tag the IP header of the encapsulated packets.

Related Information

- [About WLAN Service Template](#)

Extreme Management Center Advanced WLAN Service Settings Window (Legacy)

Use this Wireless Manager window to configure advanced WLAN Service Template settings. To access this window, click the **Advanced** button in the WLAN Service Tab.

Advanced ☒

Timeout

Idle:(pre) `5` minutes

(post) `30` minutes

Session: `0` minutes

RF

☐ Suppress SSID

☐ Enable 11h support

☐ Process client IE requests

☐ Energy save mode

☑ Radio Management (11k) support

　☐ Beacon Report

　☐ Quiet IE

Egress Filtering Mode

◉ Enforce explicitly defined "Out" rules

○ Apply "In" rules to "Out" direction traffic *

* When "In" filter rules are applied to "Out" traffic, the role of the source and destination address are reversed

Client Behavior

☐ Block MU to MU Traffic

Remote Service

☐ Remotable

Inter-WLAN Service Roaming

☑ Permit Inter-WLAN Service Roaming

Extreme-Corp

Unauthenticated Behavior

○ Discard Unauthenticated Traffic

○ Default Non-Authenticated Role

[Help]　[Close]

Timeout

Idle (pre)

Specify the amount of time in minutes that a mobile user can have a session on the Wireless Controller in pre-authenticated state with no active traffic. 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 Wireless Controller in authenticated state with no active traffic. 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 termination of the session.

RF

Suppress SSID

Select to prevent this SSID from appearing in the beacon message sent by the Wireless 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 TPC (Transmission Power Control) reports. By default this option is disabled. It is recommended that you enable this option.

Process client IE requests

Select to enable the Wireless AP to accept IE requests sent by clients via Probe Request frames and responds by including the requested IEs 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 radio management, which optimizes network performance by allowing a client to select an AP based on the number of active subscribers and overall traffic.

Beacon Report

Select to transmit a request frame from the AP to a client to request it report on beacons it has heard on all channels.

Quiet IE

Select to set a period of time where no transmission occurs on the current channel to assist in making measurements without interference.

Egress Filtering Mode

Enforce explicitly defined "Out" rules

When egress filtering mode is set to enforce explicitly defined "Out" rules, all WLAN services will enforce outbound filters on egress traffic, exactly as they are defined in the role.

Apply "In" rules to "Out" direction traffic

When egress filtering mode is set to apply "In" filter rules to "Out" direction traffic, all WLAN services will enforce that any outbound filter rules explicitly defined in the role are overridden by a set of rules created by copying each inbound filter rule and swapping the source and destination address roles in the rule. When "In" filter rules are applied to "Out" traffic, the role of the source and destination address are reversed.

Client Behavior

Block MU to MU traffic

Select the checkbox if you want to prevent two devices associated with this SSID and registered as users of the Wireless Controller, to be able to talk to each other. The blocking is enforced at the L2 (device) classification level.

Remote Service

Remotable

Select the checkbox if you want to make this service remotable.

Inter-WLAN Service Roaming

Permit Inter-WLAN Service Roaming

Select the checkbox to permit inter-WLAN service roaming.

Unauthenticated Behavior

Discard Unauthenticated Traffic

Select to drop all traffic flowing to and from an unauthenticated station. Cannot be used if any form of captive portal is the only form of authentication for the WLAN.

Default Non-Authenticated Policy
Select to apply the default non-authenticated policy to all traffic flowing to and from an unauthenticated station.

Related Information

- [About WLAN Service Template](#)

Extreme Management Center Settings Window (Legacy)

This Wireless Manager window lets you define the authentication mode settings for your WLAN Service templates. The settings in this window vary depending on the authentication mode you have selected for your template.

To access this window, select your authentication mode and then click the **Configure** button in the Add WLAN Service's Auth & Acct tab.

This Help topic provides information on configuring settings for the following authentication modes:

- Internal/Guest Portal/Guest Splash
- 802.1x with HTTP Redirection/External
- Firewall Friendly External Captive Portal

Internal/Guest Portal/Guest Splash

This section presents definitions for the various settings that can be configured for the Internal, Guest Portal, and Guest Splash authentication modes. Settings used by the different modes will vary.

Internal Authentication Mode Dialog

Guest Portal Authentication Mode Dialog

Guest Splash Authentication Mode Dialog

This section is only displayed for Guest Portal authentication mode.

Account Lifetime
Specify the number of days that a guest account will be active. A value of 0 specifies no limit to the account lifetime.

Maximum Session Lifetime
Specify the maximum number of hours that a guest session can be active. The default value of 0 does not limit the session lifetime. The session lifetime is the allowed cumulative total in hours spent on the network during the account lifetime.

User ID Prefix
Enter a prefix that will be added to all guest account user IDs. The default is Guest.

Minimum Password Length
Enter a minimum password length that will be applied to all guest accounts. The default is eight characters.

Maximum Concurrent Sessions
Specify the maximum number of concurrent guest sessions allowed. The default is unlimited.

Guest Admin Can Set Account Lifetime
Select this checkbox to allow the guest administrator to set the amount of time that this account will be active.

Login Credentials

Specify the wording that will be used for the fields in the Captive Portal where the end user will enter their login credentials.

Login Label
This label defines the field where the end user enters their user name.

Password Label
This label defines the field where the end user enters their password.

Submit Label
This label will be displayed as the text for the button to submit credentials.

Communication Options
Header URL
Enter the server location of the file to be displayed in the Header portion of the Captive Portal page. This page can be customized with logos or other

graphics to suit your organization.

Footer URL

Enter the server location of the file to be displayed in the Footer portion of the Captive Portal page.

CAUTION: If you use logos or graphics, make sure they are appropriately sized. Large logos or graphics may force the login section on the Captive Portal out of view.

Message

Enter the message that will be displayed above the Login box to greet the user. For example, the message could explain why the Captive Portal page is appearing, and provide instructions for the user. The message can be a maximum of 255 characters, including spaces.

Use HTTPS for User Connections

Select this checkbox to force Captive Portal web pages to be served securely over HTTPS (instead of HTTP) to end users on the network. Deselect this option to allow the Captive Portal to be accessed without requiring HTTPs and certificates.

Replace Gateway IP with FQDN

Specify the gateway's FQDN (Fully Qualified Domain Name) to use instead of the IP address.

Send Successful Login To

There are three Redirection options that specify where the end user is redirected following successful authentication, when the end user is allowed on the network:

- **Original destination** - If the WLAN Service is configured to send successful logins to the "original destination" and the ECP does not return the original destination then the station will be redirected to an error page.

- **Captive Portal session page** - This option lets you specify the URL for the Captive Portal session page.

- **Custom specific URL** - This option lets you specify the URL for the web page where the end user will be redirected.This would most likely be the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Specific Message URL

Enter the URL of a document that will be displayed in a text frame on the Captive Portal login page. This text frame can be used to display lengthier

messages, such as terms and conditions of use for users who have not yet logged in.

Include Attributes

If applicable, select the appropriate checkboxes in both the Header and Footer columns to include the following attributes in the message to the authentication server:

- AP Serial
- AP Name
- VNS Name
- SSID
- MAC Address

The selections influence what URL is returned in either section. For example, wireless users can be identified by which Wireless AP or which VNS they are associated with, and can be presented with a Captive Portal web page that is customized for those identifiers.

Provide button for users
Logoff
   Select the Logoff checkbox to provide users with a Logoff button that launches a pop-up logoff page, allowing users to control their logoff. When the user clicks the Logoff button, the user is disassociated and returns to the non-authenticated state.

Status Check
   Select the Status check checkbox to provide users with a Status check button that launches a pop-up window, allowing users to monitor session statistics such as system usage and time left in a session.

802.1x with HTTP Redirection/External

This section presents definitions for the various settings that can be configured for the 802.1x with HTTP Redirection and External authentication modes.

Session Control Interface

Controller Connection

External authentication server access. Port range: 32768 - 65535. For each target controller, during deployment you will be prompted to specify the IP address of one of its physical/admin topologies and port. If there is an authentication server configured for this WLAN, the external Captive Portal page on the external authentication server will send the request back to the IdentiFi Wireless Appliance to allow the appliance to continue with the RADIUS authentication and filtering.

Enable HTTPS support

Select this checkbox if you want to enable HTTPS support (TLS/SSL) for this external captive portal.

Encryption

Select the data encryption to use. Options are: None, Legacy, and AES.

Shared Secret

If you want to encrypt the information passed between the IdentiFi Wireless Appliance and the external web server, enter the password common to both the appliance and the server.

Redirection URL

Enter the URL that the wireless device user will be directed to after authentication.

NOTE: The Redirection URL does not support IPv6.

Add Controller IP & Port to redirection URL
　　Select the checkbox to enable redirection.

Special

ToS Override for NAC
　　Select this checkbox to allow ToS marking results in redirection to a captive
　　portal via a NAC server.

Firewall Friendly External Captive Portal

This section presents definitions for the various settings that can be configured
for Firewall Friendly External Captive Portal authentication mode. The settings
window for the Firewall Friendly External Captive Portal mode is shown below.

Redirect to External Captive Portal

Identity and Shared Secret
　　Identity and shared secret are optional. They must be provided if the ECP is
　　going to sign its redirection responses and wants the controller to sign its
　　redirection responses. The identity must be a printable (non-control code)

ASCII alphanumeric string. The shared secret should be a printable (non-control code) ASCII string. It should have a length of between 16 and 255 characters. It can contain slashes, braces and other printable ASCII symbols. As the name "shared secret" implies, exactly the same key must be configured on the ECP and associated with the same identity.

These two fields play a crucial role in signature generation. The identity field must be included in any signed redirected web request that redirects a user from ECP to the controller or vice versa. The identity tells the receiver which shared secret to use to validate the message signature.

The identity field and shared secret work together as a pair. Different WLAN Services on one controller can have the same identity configured, in which case the WLAN Services must have the same shared secret.

Redirection URL

The redirection URL is the URL that stations will have their HTTP traffic redirected to. This is a mandatory field and should point to a page, script or program served by the ECP. Both HTTP and HTTPS are supported.

The redirection URL will have some parameters appended to it when it is received by the ECP. All information communicated with the ECP will be part of the redirection URL query string. The minimum information included in the URL are a token, a WLAN identifier and the original URL that the station was trying to access when it was redirected to the ECP.

- The token is an identifier for the user-session. It must be included as a query string parameter in all ECP redirections back to the controller.

- The WLAN identifier helps the controller determine how to process the redirect back from the ECP. It must be included in the redirection sent by the ECP to the controller's web server.

- The original URL that the station was trying to access when it was redirected may or may not be important. If the administrator wants all authenticated users to end the login sequence on one specific page (such as the site's news page) then the original URL can be ignored by the ECP. If the administrator wants the user to be redirected to a session management page after a successful login or if he wants the user to be sent to the original URL then the ECP must save the original URL and include it in the redirection that causes the user's browser to return back to the controller.

NOTE: The following (optional) attributes can be sent by the Controller to the ECP via Browser Redirection.

EWC IP & Port
Select this checkbox to include the controller's address on the topology (VLAN) to which the user is assigned. The controller can include its IP address and port in the redirection URL. This is optional, but necessary if the ECP interacts with more than one controller. Without these fields the ECP may not be able to compose the correct redirection URL to cause a station to complete authentication on the correct controller. Only IPv4 addresses are supported.

Unlike standard ECP, the administrator does not directly configure the controller IP address and port to which the ECP should redirect stations. Standard ECP makes use of a separate connection that is used by the ECP to send session control messages to the controller. FF-ECP does not have this connection because control messages are relayed from the ECP to the controller via redirecting the station's browser.

Since the station's browser conveys the commands to the controller the station must have easy access to the controller interface and port that will receive the redirection. This will be the controller's address on the topology (VLAN) to which the user is assigned. The address to use is only known once a VNS based on the WLAN Service is fully configured.

Replace EWC IP with EWC FQDN
Sometimes it is convenient for the ECP to be able to redirect stations back to an FQDN belonging to a controller. This is necessary to avoid certificate warnings when the certificate contains FQDNs for identity instead of IP addresses. The "EWC IP and Port" option normally adds the IP address and port on the controller that the ECP should redirect clients to. If "EWC IP and Port" is enabled and the FQDN field is populated with a valid FQDN the controller will put the provided FQDN and port into the redirection it sends to the station. This option only takes effect when the "EWC IP and Port" option is enabled.

AP name & serial number
Select this checkbox to include the name and serial number of the AP associated with this station. Can be useful if the ECP needs to behave differently depending on the location of the station being authenticated.

Associated BSSID
Select this checkbox to include the Basic Service Set Identifier (BSSID) to which the station being authenticated has associated. It is the MAC address belonging to the AP to which the station has associated. The BSSID is the same identifier that the controller puts in the Called-Station-ID RADIUS TLV sent in Access-Requests and RADIUS accounting messages. The associated

BSSID will be sent in the form of a 12 character ASCII-encoded lowercase hex string, for example: "00112233aabb".

VNS Name
Select this checkbox to include the name of the VNS associated with the SSID.

SSID
Select this checkbox to include the SSID that identifies the WLAN service for the wireless controller.

Station's MAC Address
This attribute uniquely and globally identifies the station. More specifically, this is the MAC address of the station's wireless interface that associated to the BSSID. This holds the same value that the controller puts in the Calling-Station-Id RADIUS attribute. The station MAC address will be sent in the form of a 12 character ASCII-encoded lowercase hex string, for example: "00112233aabb".

Currently assigned role
This attribute contains the name of the access control role assigned to the station at the time its browser was redirected to the ECP. The contents of this attribute match the contents of the Siemens RADIUS VSA called "Siemens-Policy-Name".

Containment VLAN (if any) of assigned role
If the default action of the Currently Assigned Role is "Contain to VLAN" then this contains the name of the topology/VLAN to which the station's traffic is contained by default. Roles need not have a Contain to VLAN default action, in which case this attribute would be empty, even if requested.

Timestamp
Select this checkbox to include the time on the controller (in UTC seconds elapsed since 1970-01-01 00:00:00) at which the HTTP request that was redirected to the ECP was received. The timestamp will be included if the controller is configured to sign the redirection to the ECP, even if it was not explicitly requested. The timestamp is useful for preventing replay attacks of recorded redirected requests.

Signature
Select this checkbox to have the controller compute a secure hash over portions of the redirection response. Even if not explicitly requested, the response will include a timestamp. Requires the user to configure Shared Secret and Identity properties.

The identity will be included in the redirect to the ECP. The ECP can use this to look up the appropriate shared secret in order to validate the signature.

Selecting the timestamp and signature options does not cause the controller to expect signatures on the redirects from the ECP. However if a WLAN Service that uses FF-ECP is not configured with at least one RADIUS authentication server then the redirections from the FF-ECP to the controller must be signed and time stamped.

Redirect From External Captive Portal
Use HTTPS for User Connections
This setting controls whether the controller listens for redirects at port 443 or port 80 and whether it expects to receive redirects from the ECP as HTTPS or HTTP.

The default is to use HTTPS. This is the most secure option. The controller has a self-signed certificate that it will use by default for HTTPS. However, most browsers will immediately warn the user that they are being redirected to a site with a self-signed certificate. If this service is to be used by large numbers of users or by casual users it is best to obtain a certificate from a CA that is trusted by all browser vendors. An administrator running multiple controllers with FF-ECP can obtain a wildcard certificate that covers all the interfaces of all the controllers.

If a third party certificate is installed, it must be installed on the topology that stations have direct access to (typically either the WLAN Service's default topology/VLAN or the station's role's default action's containment VLAN).

Send Successful Login To
There are three Redirection options that specify where the end user is redirected following successful authentication, when the end user is allowed on the network:

- **Original destination** - This option redirects the end user to the web page they originally requested when they connected to the network. If the WLAN Service is configured to send successful logins to the "original destination" and the ECP does not return the original destination then the station will be redirected to an error page.

- **Captive Portal session page** - This page contains controls to tell how long the user's session has lasted and to gracefully terminate the user's session. It can also contain a link to the original URL the browser was trying to receive when it was redirected. The "original URL" option will only work if the ECP sends to the controller the original URL ("dest" parameter) that the

controller sent to the ECP in the initial redirect. If the ECP does not return the original destination URL in the redirect to the controller and the WLAN Service is configured to redirect the station to "Captive Portal Session Page" the user will be redirected to that page, but it will not contain a link to the original destination.

- **Custom specific URL** - This option lets you specify the URL for the web page where the end user will be redirected.This would most likely be the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Related Information

- [About WLAN Service Template](#)

About Role Templates in Extreme Management Center (Legacy)

A Role defines the binding of a topology (VLAN), Class of Service, and filter rules that should be applied to the traffic of a station. Roles don't need to be fully specified; unspecified attributes are retained by the user or inherited from the Global Role definitions on the Wireless Controller.

This Help topic includes the following information:

- [Creating a Role Configuration Template](#)
- [Migrating Legacy Role Templates](#)
- [Using Policy Manager to Create Role Templates](#)
- [Viewing Roles Summary Information](#)
- [Viewing Detail Information About a Role](#)
- [Viewing Legacy Summary Information](#)
- [Viewing Detail Information About a Legacy Role](#)

Creating a Role Configuration Template

Wireless Manager no longer supports the configuration of Roles (see [Legacy Template Migration Notice](#)).

Migrating Legacy Role Templates

If you have any legacy Role templates, they must be migrated within 30 days otherwise support will be terminated.

To migrate existing Role Templates:

1. Deploy your templates to the managed wireless controllers.

2. Using Policy Manager, assign your wireless controllers to a Policy domain and import their configuration. Select File > Import > Policy Configuration from Device.

3. From the Import from Device wizard, you must specify whether to import

roles, rules, and/or Class of Services.

4. Save your changes.

5. Modify your Wireless Manager templates as needed to reference the newly created Role and CoS templates automatically imported from Policy Manager.

6. Remove the legacy templates.

- You can either delete the templates one-by-one or for your convenience use the following buttons displayed in the Legacy Template Migration dialog:

  - Brute-Force Cleanup – Deletes all legacy templates whether or not they are referenced by other templates. VNS templates may become "Incomplete".

  - Best-Effort Cleanup – Deletes all legacy templates not referenced by other templates.

- If "Brute-Force Cleanup" results in a VNS becoming "Incomplete", it will be displayed in the Conflict Resolution wizard as a reminder for you to complete its definition and to specify a Non-Authenticated role for it.

- Please note these cleanup operations will even remove the legacy predefined CoS: Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, RTP/Voice/Video, and High Priority. However, upon synchronization with Policy Manager they will be automatically re-created, and will be consistent with their Policy Manager counterparts.

Using Policy Manager to Create Role Templates

If you are using Policy Manager, after you save the configuration for a particular domain that includes Wireless Controllers, Wireless Manager will automatically create for you those Roles defined in the domain. Since a Role in Policy Manager can have different definitions in different domains, in Wireless Manager the Navigation Tree shows a single Role, which when clicked, displays a separate tab for each domain specific version of the Role.

Roles created on behalf of Policy Manager follow these guidelines:

- PM-Roles are located under the Templates tab > Roles > Roles section of the Navigation Tree. Roles created using Wireless Manager, either manually or by cloning an existing Role Template or deployed Role, are located

under the Templates tab > Roles > Roles > Legacy.

- PM-Roles can be easily identified in drop down lists (for example, for selection in a VNS) since their names include the name of the Policy Manager domain from which they were created.

- PM-Roles cannot be edited from within Wireless Manager except for configuring their Point of Presence. For more information on Deploying the Point of Presence Wizard, see [Creating, Scheduling, and Deploying Tasks](#).

- PM-Roles cannot be deleted by the user. A PM-Role will be automatically deleted from Wireless Manager when it is either deleted from all those domains (with assigned Wireless Controllers) where it is defined, or all the Wireless Controllers are removed from those domains where it is defined. If a PM-Role exists in multiple domains, and instead the Role is deleted from just one domain (with assigned Wireless Controllers) where it is defined, or all the Wireless Controllers are removed from that domain, then the corresponding domain specific version of that Role is deleted from Wireless Manager. If the domain specific version of the PM-Role was being referenced by a VNS template, then that template is marked "Incomplete" and must be completed before it can be deployed.

- PM-Roles are not deployable by themselves, but can be referenced in the deployment of VNS. During the deployment of a VNS template referencing PM-roles, the user can now select the option 'Enforce using Policy Manager' to have Wireless Manager trigger Policy Manager to enforce the domain configuration on any target controllers referenced by the deployment task. If this option is not selected, Wireless Manager will assume that these PM-roles already exist on the target Wireless Controllers. In general this is a valid assumption since the user, most likely, has already used Policy Manager to "Enforce Role Set" for the domain where these Wireless Controllers reside. In the unlikely scenario these PM-roles don't yet exist on the target Wireless Controllers, Wireless Manager will fail the deployment with a suitable error message, and you can correct the problem from Wireless Manager by selecting the option 'Enforce using Policy Manager' during deployment or from Policy Manager using "Enforce Role Set".

- The Status for these PM-Roles are blank. PM-Roles are not audited by Wireless Manager. Instead, Policy Manager detects and reports any discrepancies between the current Role set of a domain and the Roles defined on the Wireless Controllers in the domain. Wireless Manager however, will verify that a VNS is referencing the correct PM-Roles on the target Wireless Controllers.

For more information about how to create Roles in Policy Manager, refer to the NetSight Policy Manager User Guide.

Viewing Roles Summary Information

You can view summary information about PM-Roles currently defined in Wireless Manager from the Summary for PM-Roles page. From this page, you can see at a glance the set of Policy Manager domains where a particular PM-Role is defined.

To view summary information for PM-Roles:

1. Click the Templates tab.

2. In left-hand pane, click Roles and select the Roles folder. The Summary for Roles page displays the Policy domains for each Role.

Viewing Detail Information About a Role

To view information about a configured Role:

1. Click the Templates tab.

2. In left-hand pane, click Roles. Expand the Roles folder and select a Role. The Roles Details page displays.

NOTE: PM roles can have different definitions in different domains.
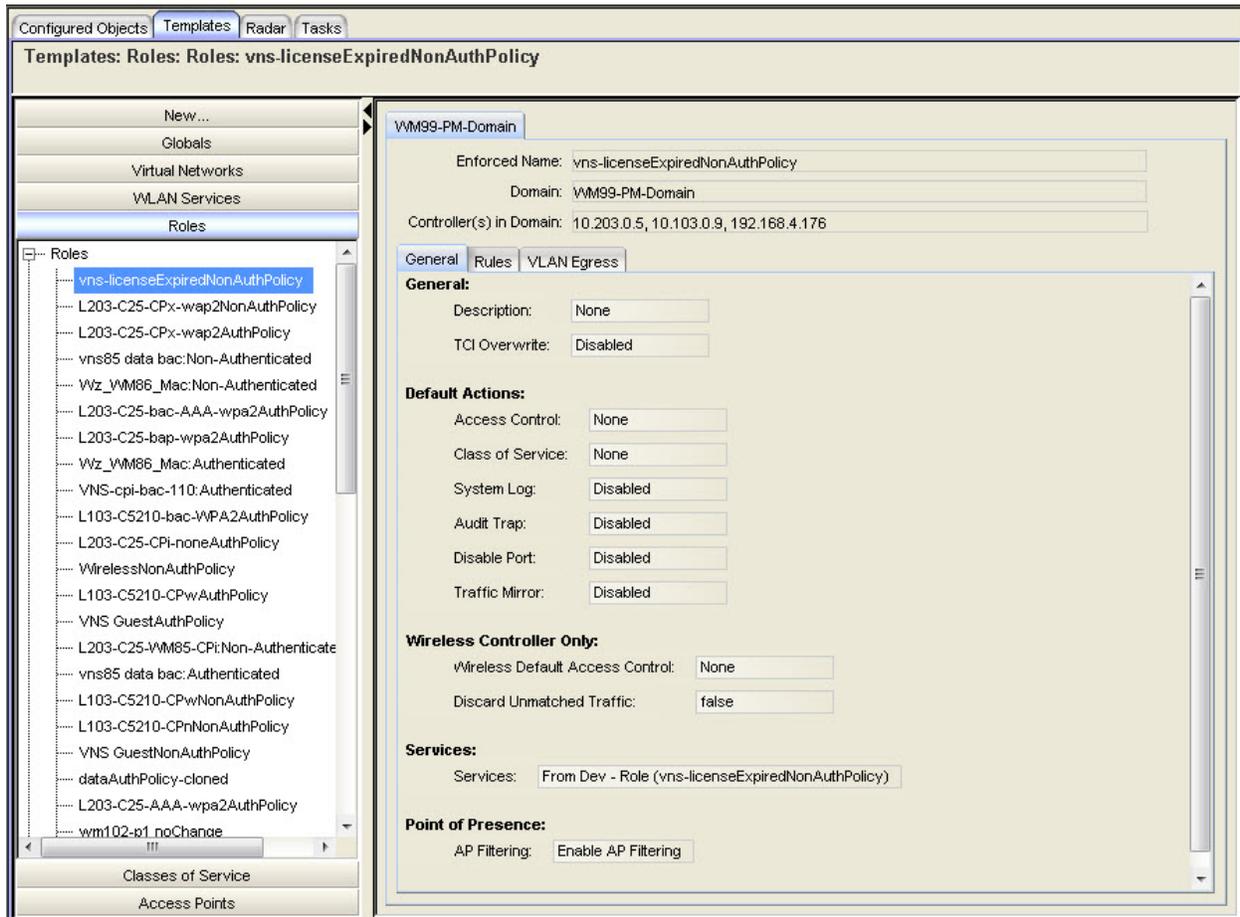
The following list describes the information available on the Roles Details page.

Default Policy Domain Tab

Enforced Name

Name of this Role if it were deployed to a Wireless Controller in that domain.

Domain

Domain name.

Controller(s) in Domain

IP addresses of all those controllers assigned to the specified Policy Manager domain.

General Tab

Please refer to the Policy Manager User Guide for information.

Rules Tab

Read-only view of the policy rules assigned to the role, with links to referenced PM CoS and/or PM topologies. Please refer to the *Policy Manager User Guide* for information.

VLAN Egress Tab

Read-only view of the Egress VLANs assigned to the role with links to referenced PM topologies. Please refer to the *Policy Manager User Guide* for information.

Viewing Legacy Summary Information

Wireless Manager no longer supports the configuration of Roles (see Legacy Template Migration Notice).

To view information about configured Legacy Roles:

1. Click the Templates tab.

2. In left-hand pane, click Roles. Expand the Roles folder and select Legacy. The Summary for Legacy Roles page displays.
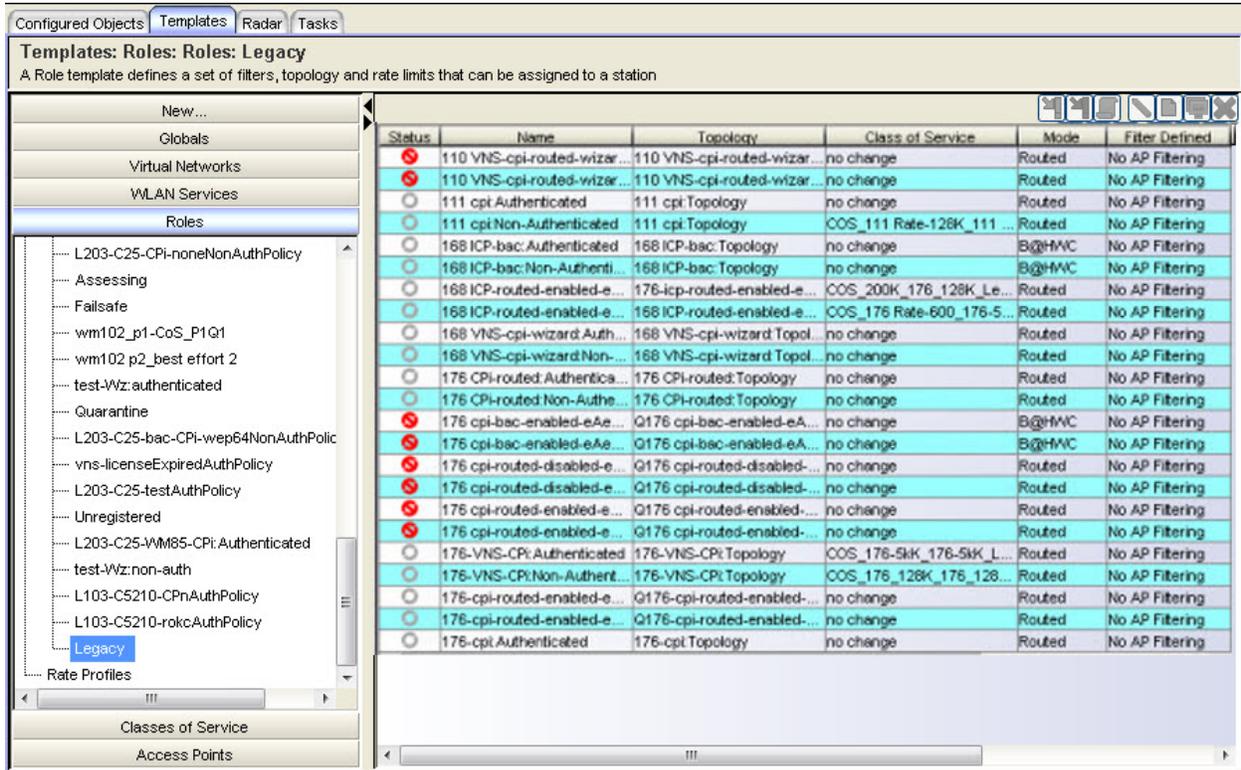
The following list describes the information available on the Summary for Legacy Roles page.

Status

    Status of this Role. Options include:

    ⬤ Deployed, ⭕ Not Deployed, 🚫 Deployed but not synchronized to the network

    🚫 Deployed but some templates not synchronized.

Name

    Name assigned to this Role.

Topology

    Topology assigned to this Role.

Class of Service

    Class of Service assigned to this Role.

Mode

    The mode of operation of the topology assigned to this Role. Values are: Routed, B@AP, or B@EWC.

Filter Defined
Indicates whether AP Filtering or Custom AP Filtering is enabled.

Controllers
List of Wireless Controllers to which this Role is deployed.

Toolbar Buttons
For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Viewing Detail Information About a Legacy Role

Wireless Manager no longer supports the configuration of Roles (see [Legacy Template Migration Notice](#)).

To view information about a Legacy Role:

1. Click the Templates tab.

2. In left-hand pane, click Roles. Expand the Roles folder and select a Legacy Role. The Legacy Role Details page displays with the Template Properties tab active. For more information about the fields on this tab, see the [Template Properties Tab](#) Help topic.

The following sections describe the information available on the Role Template Configuration tabs.

VLAN and Class of Service Tab
Name
Name of this Role.

Assigned Topology
Select a Topology to assign to this Role from the list.

Default Class of Service
Select the Class of Service to assign to this Role. Options include:

- no change - The Class of Service of the prior Role Template is used.

- No CoS - No rate limiting, no TXQ assignment, no Marking.

- Predefined CoS for PM: Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, RTP/Voice/Video, High Priority.

- Classes of Service listed alphabetically.

Filters Rules Tab
Enable AP Filtering
Select the checkbox to enable filtering on the APs.

Inherit filter rules

Select the checkbox to inherit filter rules from currently applied Role.

Rule

Options include:

- U – The filter has user-defined rules
- D – The default filter

In

Identifies the rule that applies to incoming traffic. You can change this setting using the drop-down menu. Options include: Destination (dest), Source (src), None, and Both.

Out

Identifies the rule that applies to outgoing traffic. You can change this setting using the drop-down menu. Options include: Destination (dest), Source (src), None, and Both.

IP:Port

The IP address and port on the Wireless Controller or AP to which this filter applies.

Protocol

The protocol to which this filter applies.

Priority

This is the 802.1p value of this filter.

ToS/DSCP

This is the ToS/DSCP marking value of this filter.

Access

Allow or Deny access.

CoS

This is the Class of Service assigned to this filter.

Up

Click to move the selected filter up in the list.

Down

Click to move the selected filter down in the list.

Add

Click to add a new filter rule. The following fields appear in the Add Filter dialog:

Direction

In Filter - Options include: Destination (dest), Source (src), None, and Both.

Out Filter - Same options as the In Filter except it refers to outgoing traffic.

Classification

IP/Subnet: The IP address and subnet to which this filter applies.

Port: Port designation on the IP address.

Protocol: In the Protocol drop-down list, click the applicable protocol. The default is N/A.

ToS/DSCP Marking

Priority

Action

Access Control

Class of Service

OK: Click to add the filter rule to the filter group. The information displays in the filter rule table.

Cancel: Click to discard your changes.

Edit
Click to edit the selected filter.

Delete
Click to remove the selected filter from the list.

Per Controller Settings Tab
Assigned Topology
Includes a link to the Topology assigned to this Role, so that you can view its per-Wireless Controller customizations.

About Rate Profiles in Extreme Management Center (Legacy)

A rate profile can limit the maximum amount of throughput that is available to a station. See Legacy Template Migration Notice.

This Help topic includes the following information:

- Viewing Summary Information About All Rate Profiles
- Viewing Detail Information About a Rate Profile

Viewing Summary Information About All Rate Profiles

You can view summary information about rate profile configurations currently defined in Wireless Manager by accessing the Rate Profile Summary page. From this page, you can also perform the following tasks:

- Edit, clone, or delete an existing rate profiles definition.
- Create tasks to deploy a rate profile.
- Export an rate profile configuration to the CLI.
- Create new rate profile definition.

To view information about configured rate profiles:

1. Click the Templates tab.
2. In left-hand pane, click Roles, and then click Rate Profiles. The Rate Profiles Summary page displays.

The following list describes the information available on the Rate Profile Summary page.

Status

Options include:

⬤ Deployed, ◯ Not Deployed, 🚫 Deployed but not synchronized to the network

Name

Name assigned to this rate profile.

Average Rate (Kbps)

Data transfer rate in Kbps assigned to this rate profile.

Used by Policy

Policies that use this rate profile.

Controllers

Wireless Controllers that use this rate profile.

Toolbar Buttons

For a description of common toolbar buttons see Context-Sensitive Toolbar.

Viewing Detail Information About a Rate Profile

To view information about a Rate Profile:

1. Click the Templates tab.

2. In left-hand pane, click Roles. Expand the Rate Profiles folder and select a Rate Profile. The Rate Profiles Details page displays with the Template Properties tab active. For more information about the fields on this tab, see the [Template Properties Tab](#) Help topic.

3. Click on the Rate Profile Properties tab to view read-only properties for the Profile.
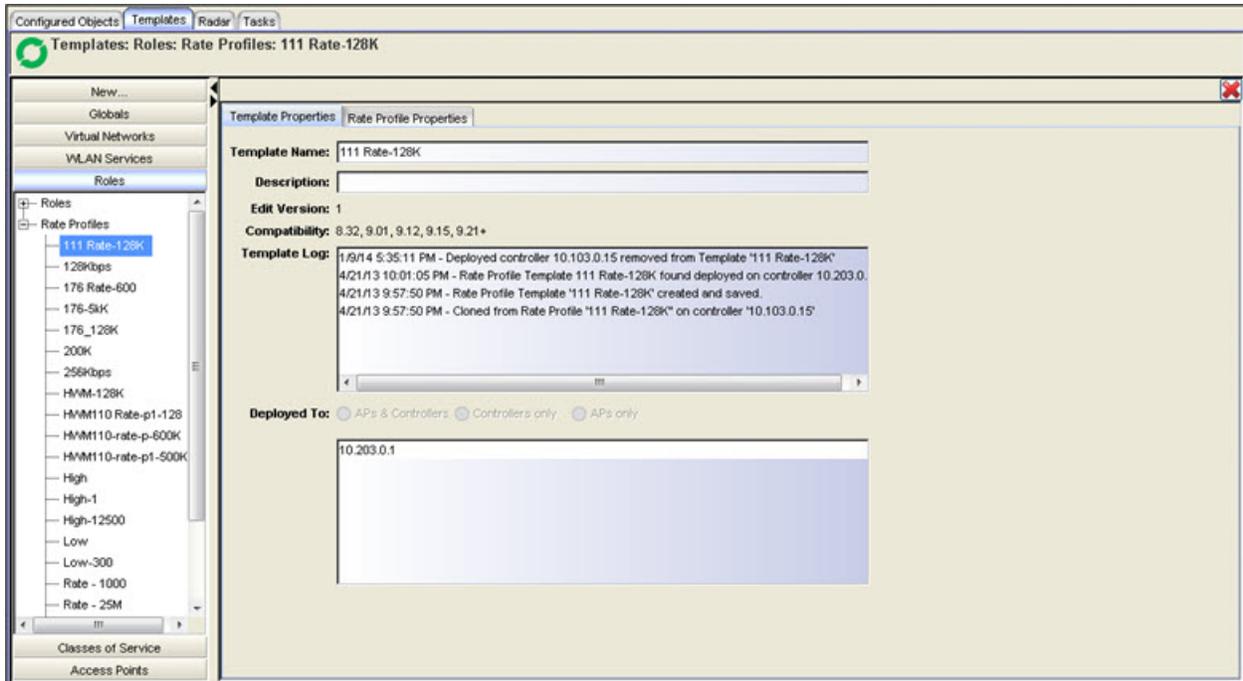
About AP Profiles in Extreme Management Center (Legacy)

An AP Profile is a template that contains a set of AP configuration attributes. You can assign an AP Profile to one or more APs in your network.

This Help topic includes the following information:

- [Creating an AP Profile Template](#)
- [Viewing Summary Information About All AP Profiles](#)

Creating an AP Profile Template

You can create an AP Profile template either manually, or by cloning an existing template or an AP configuration. You can also assign an AP Profile to a Wireless Controller as one of its default AP Profiles. (A Wireless Controller has one default AP Profile for each family of compatible hardware types.)

Manually Creating an AP Profile

To manually create an AP Profile template or configuration:

1. Click the Templates tab.

2. In the left pane, click New, expand the New folder and click Add AP Profile.

3. The Access Point Configuration page displays with the Template Properties tab active.
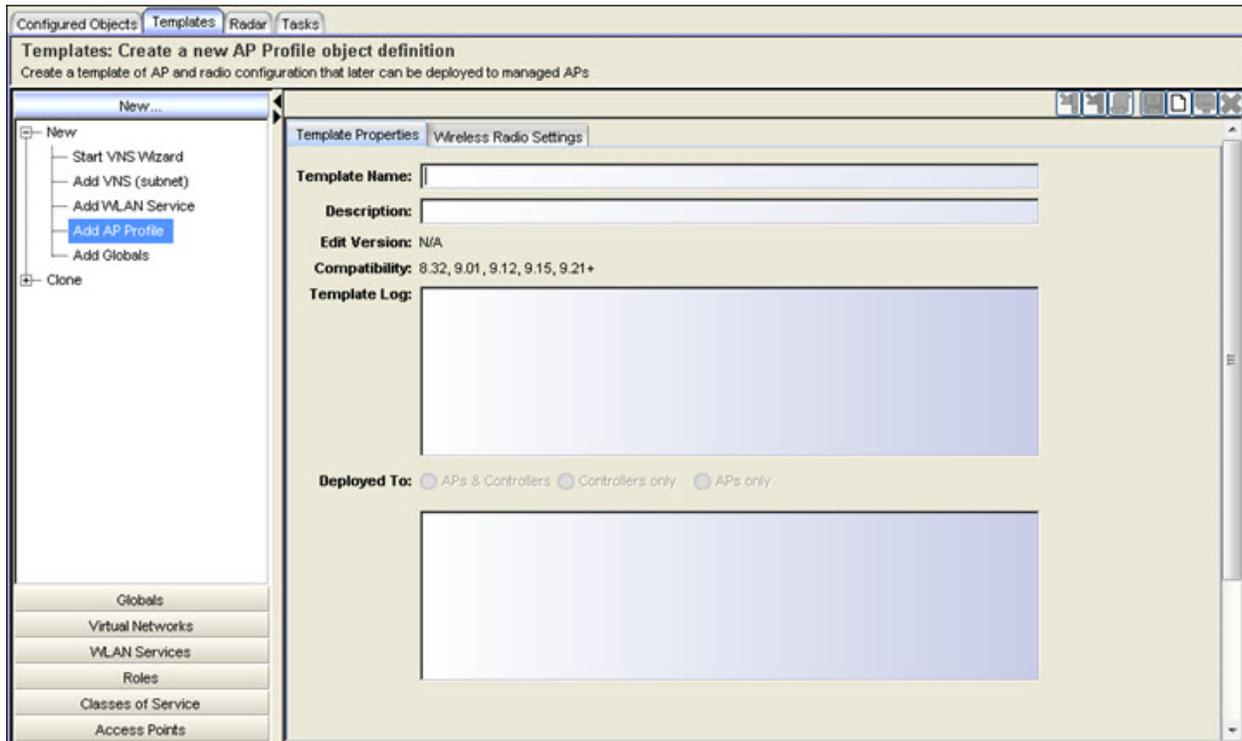
4. Enter a name for the new template. Enter a template description, if desired. For more information about the fields on this tab, see the [Template Properties Tab](#) Help topic.

5. Click on the Wireless Radio Settings tab.

6. Select the AP Profile Type. Options include: ABG capable, ABGN capable, Dual Band ABG capable, RoamAbout APs (thin mode), AP37xx W78xC, AP38xx, and AP3801.

7. Select the Regulatory Domain. This is the geographic location where the AP will operate. In general, for a template to be deployed successfully, the regulatory domain in the template must match the regulatory domain in the Wireless Controller's license.

8. Select the Hardware Type. Options change depending on the AP Profile Type selected. For APs with an external antenna in the hardware type, professional installation is enabled.

9. Use the AP Properties and Radio Settings sub-tabs to configure additional settings. The two tabs are described below.

AP Properties Tab

Location

Defines the Location of the Wireless AP. Select a new Location or choose from any Location already configured in an AP reported by a Wireless Controller, or in another AP Profile template. The default Location is No Change. The Location property supports UTF8 encoding and is only configurable for APs; it is not a property of any AP Default Settings on the Wireless Controller.

Policy Zone

Defines the location-based Policy Zone for the specified AP. Multiple APs can and will have the same Policy Zone. Select a new Policy Zone or choose from any Policy Zone already configured in an AP reported by a Wireless Controller, or in another AP Profile template. The default Policy Zone is No Change. The Policy Zone property is only configurable for APs on 8.11+ Wireless Controllers; it is not a property of any AP Default Settings on the controller.

AP Environment

Options are Indoor and Outdoor.

Role

Select either Access Point, Sensor, or Do not change. Once the AP is configured as a Sensor, the AP is no longer managed by the Wireless Controller.

Country

Select the Country of operation within the specified Regulatory Domain for this AP Profile.

Tunnel MTU

Enter a static MTU value, from 600 to 1500. 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

Click to Enable or Disable Link Aggregation Control Protocol (LACP) for this AP. LACP allows two or more Ethernet ports to be dynamically aggregated. On AP38xx and AP3801, LACP negotiates the two Ethernet ports into a single Link Aggregate Group (LAG). When operating as a LAG, by default the AP distributes the uplink traffic between the two Ethernet ports such that

all traffic from each radio goes through separate ports. This settings applies to Wireless Controllers running 9.01 or later.

Ethernet Speed

Options include: Auto, 10Mbps, and 100Mbps.

Ethernet Mode

Options include: Full-Duplex, Half-Duplex

AP Properties Tab - Professional Install Button

Antenna Types

Radio 1 and Radio 2 (Left, Middle, and Right) - Select the Antenna Types for the AP hardware type to which this AP Profile has been restricted.

Radio1 Attenuation

Select an attenuation level from the drop-down list.

Radio2 Attenuation

Select an attenuation level from the drop-down list.

AP Properties Tab - Advanced Button

Poll Timeout(s)

Type the timeout value, in seconds, for the Wireless AP to re-establish the link with the Wireless Controller if it (Wireless AP) does not get an answer to its polling. The default value is 10 seconds.

Secure Tunnel

Select the desired Secure Tunnel mode from the drop-down list:

- **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.

NOTE: Changing a Secure Tunnel mode will automatically disconnect and reconnect the AP.

Secure Tunnel Lifetime [hours]
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
later. Default is 0 (hours).

NOTE: Changing the Secure Tunnel Lifetime setting will not cause any AP disruption.

Telnet/SSH Access
Click to enable or disable Telnet / SSH for access to the Wireless AP.

Maintain Client Sessions in Event of Poll Failure
Select this option (if using a bridged at AP VNS) if the Wireless AP should
remain active if a link loss with the Wireless Controller occurs. This option is
enabled by default.

Restart Service without Controller
Select this option (if using a bridged at AP VNS) to ensure the Wireless AP's
radios continue providing service if the Wireless AP's connection to the
Wireless Controller is lost. If this option is enabled, it allows the Wireless AP
to start a bridged at AP VNS even in the absence of a Wireless Controller.

Use Broadcast for Dissociation
Select this option if you want the Wireless AP to use broadcast disassociation
when disconnecting all clients, instead of disassociating each client one by
one. This option is disabled by default.

LLDP
Select to enable or disable the Wireless AP from broadcasting LLDP
information. This option is disabled by default.

Announcement Interval(s)
If LLDP is enabled, type how often the Wireless AP advertises its information
by sending a new LLDP packet. This value is measured in seconds. If there
are no changes to the Wireless AP configuration that impact the LLDP
information, the Wireless AP sends a new LLDP packet according to this
schedule.

Announcement Delay(s)
If LLDP is enabled, type the announcement delay. This value is measured in
seconds. If a change to the Wireless AP configuration occurs that impacts the

LLDP information, the Wireless 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.

Time to Live(s)
The Time to Live value cannot be directly edited. The Time to Live value is calculated as four times the Announcement Interval value.

IP Multicast Assembly
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. This option is disabled by default.

Balanced Channel List Power
When selected, the controller will automatically reduce the configured 'Max Tx Power' to the lesser of the configured value or the minimum of the 'Max Tx Power' values allowed for the AP (by regulatory compliance) over the selected channel plan. When unselected, the controller will automatically reduce the configured 'Max Tx Power' to the lesser of the configured value or the maximum of the 'Max Tx Power' values allowed for the AP (by regulatory compliance) over the selected channel plan.

LED
Options include: Off, WDS Signal Strength, Identify, Normal.

Location-Based Service
Click to enable or disable location based service on this Wireless AP. Location-based service allows you to use this Wireless AP with an AeroScout solution.

Radio Settings Tab

Admin Mode
Select On to enable the radio; select Off to disable the radio.

Radio Mode
Radio 1 Options are: a, a/n, a/n/ac, n-strict.
Radio 2 Options are: b, g, b/g, g/n, b/g/n, n-strict

Channel Width
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 802.11 a/b/g radio protocols.

— 802.11n clients that do not support the 40 MHz frequency can use 20MHz or the 802.11 a/b/g radio protocols.

— Non-802.11n clients, beacons, and multicasts use the 802.11 a/b/g radio protocols.

80 MHz Channel bonding is enabled:

— 802.11ac clients that support the 80MHz frequency.

Auto — Channel bonding is automatically enabled or disabled, switching between 20MHz and 40MHz, 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.

New Channel Representation

20 MHZ channels are identified with the channel number or central frequency in MHz (for example, channel number 40 is 5200 MHz)

40 MHz channels contain two 20 MHz channels and either can be primary given a 40 MHz channel occupying 5180 and 5200 MHz, it can be represented as 36+ when the primary channel is 5180 or 40- when the primary channel is 5200

With the introduction of 11ac and support for 80 MHz-wide channels we needed a better way to identify them. The channel up/down notation may be sufficient for 40 MHz channel bonding, but with 80 MHz-wide channels there are more than two options to select the primary channel.

Channel Representation

Channel	80 MHz Channel	Short Notation	Long Notation
5180	(5180, 5200, 5220, 5240)	36/80	36: ([5180], 5200, 5220, 5240)
5200		36 +1/80	40: (5180, [5200], 5220, 5240)
5220		36 +2/80	44: (5180, 5200, [5220], 5240)
5240		36 +3/80	48: (5180, 5200, 5220, [5240])

Short Notation is the lowest 20 MHz channel # + 0-based offset of the primary channel / channel width.

Long Notation is the primary channel followed by the center frequencies of the contained 20 MHz channels with the primary channel frequency enclosed in [ ].

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 Wireless APs.

Guard Interval

Click a guard interval, Long or Short, when a 40 MHz channel is used. It is recommended that you use a short guard interval in small rooms (for example, a small office space) and a long guard interval in large rooms (for example, a conference hall).

Channel Plan - Radio 1

If ACS is enabled, you can define a channel plan for the Wireless 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:

- **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 available when there is at least one DFS channel supported for the selected country.

Channel Plan - Radio 2

If ACS is enabled, you can define a channel plan for the Wireless 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:

- **3 Channel Plan** — ACS will scan 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 will scan 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 will scan 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.

Auto Transmit Power Control

Select to enable ATPC. ATPC automatically adapts transmission power signals according to the coverage provided by the Wireless APs. After a period of time, the system will stabilize itself based on the RF coverage of your Wireless APs. The APs should be part of the same RF Domain to function properly.

Max Tx Power

Click the maximum Tx power level to which the range of transmit power can be adjusted. For an AP Profile that is not restricted to a particular hardware type, it is recommended that you select 24 dBm to use the entire range of potential Tx power.

Min Tx Power

If ATPC is enabled, click the minimum Tx power level to which the range of transmit power can be adjusted. It is recommended that you select the lowest value available to use the entire range of potential Tx power.

Auto Tx Power Ctrl Adjust

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 your initial configuration. If you have an RF plan that recommends Tx power levels for each Wireless 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.

Antenna Selection

Click the antenna, or antenna combination, you want to configure on this radio. When you configure the Wireless 802.11n AP to use specific antennas, the transmission power is recalculated; the Current Tx Power Level value for the radio is automatically adjusted to reflect the recent antenna configuration. It takes approximately 30 seconds for the change to the Current Tx Power Level value to be reflected in the ExtremeWireless Wireless Assistant. Also, the radio is reset causing client connections on this radio to be lost.

NOTE: Antenna Selection is not applicable to the AP3605, 4102, or outdoor AP models.

Radio Settings Tab - Professional Install Button

Antenna Types

Radio 1 and Radio 2 (Left, Middle, and Right) - Select the Antenna Types for the AP hardware type to which this AP Profile has been restricted.

Radio1 Attenuation

Select an attenuation level from the drop-down list.

Radio2 Attenuation

Select an attenuation level from the drop-down list.

Radio Settings Tab - Advanced Button

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 (ms)

Type the desired time, in milliseconds, between beacon transmissions. The default value is 100 milliseconds.

RTS/CTS (Bytes)

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.

Fragmentation Threshold (Bytes)

Type the fragment size threshold, in bytes, above which the packets will be fragmented by the Wireless AP prior to transmission. The default value is 2346, which means all packets are sent unfragmented. Reduce this value only if necessary.

Max% Non-Unicast Traffic per Beacon Period

Enter the maximum percentage of time that the AP will transmit 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.

Maximum Distance (m)

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 acknowledgment 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.

Optimized Multicast for Power Save
Click to enable the transmission of multicast packets from CABQ using TXOP of 3 msec. (same as video).

Adaptable rate for Multicast
Click to enable the multicast transmit rate to be the minimum unicast transmit rate of all clients on the VLAN (topology).

Multicast to Unicast delivery
Click to enable the transmission of multicast traffic as unicast packets for increased speed.

Dynamic Channel Selection
To enable Dynamic Channel Selection, click one of the following:

- **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 Wireless AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Wireless AP to operate on.

Minimum Basic Rate
Click a minimum basic rate: 1 Mbps, 2Mbps, 5.5Mbps, 11Mbps.

DCS Noise Threshold
Type the noise interference level, measured in dBm, after which ACS will scan for a new operating channel for the Wireless AP if the threshold is exceeded.

DCS Channel Occupancy Threshold
Type the channel utilization level, measured as a percentage, above which Dynamic Channel Selection will be engaged.

DCS Update Period
Type the time, measured in minutes that determines the period during which the Wireless AP averages the DCS Noise Threshold and DCS Channel Occupancy Threshold measurements. If either one of these thresholds is exceeded, then the Wireless AP will trigger ACS.

Probe Suppression
Suppresses client probing, which causes multiple APs to respond unnecessarily in high-density deployments.

Force Disassociate
Disassociates clients from an AP when five dBm below the suppression threshold. This allows them to automatically reconnect to a better AP.

RSS Threshold
Sets the minimum RSS threshold, below which clients cannot associate to the AP.

Receive Diversity
Click Best for the best signal from both antennas, or Left or Right to choose either of the two diversity 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.

Transmit Diversity
Click Alternate for the best signal from both antennas, or Left or Right to choose either of the two diversity 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, It is recommended that you use either Left or Right for Tx Diversity. If only one antennae is connected, use the corresponding Left or Right diversity setting. Do not use Alternate if two identical antennas are not used.

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 AP. Click Long if compatibility with pre-11b clients is required.

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: CTSOnly 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.

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. 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.

40 MHz Channel Busy Threshold

Type the extension channel threshold percentage, which if exceeded, will disable transmissions on the extension channel (40 MHz).

AMSDU

Click an aggregate MSDU mode: Enabled or Disabled. Aggregate MSDU increases the maximum frame transmission size.

AMPDU

Click an aggregate MPDU mode: Enabled or Disabled. Aggregate MPDU provides a significant improvement in throughput.

AMPDU 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 acknowledgment, provides acknowledgment of a group of frames instead of a single frame. ADDBA Support must be enabled if Aggregate APDU is enable.

LDPC

Click a Low-Density Parity-Check (LDPC) mode: Enabled or Disabled. LDPC increases the reliability of the transmission resulting in a 2dB increased performance compared to traditional 11n coding.

NOTE: Only available on 8.11+ Wireless Controllers for AP37xx, W78xC, AP38xx, and AP3801 APs.

STBC
Click a Space Time Block Coding (STBC) mode: Enabled or Disabled. STBC is a simple open loop transmit diversity scheme. When enabled, STBC configuration is 2x1 (one spatial stream split into two space-time streams). TXBF will override STBC if both are enabled for single stream rates.

NOTE: Only available on 8.11+ Wireless Controllers for AP37xx, W78xC, AP38xx, and AP3801 APs.

TXBF
Click a Transmit Beam Forming (TXBF) mode: Enabled or Disabled. Tx Beam Forming focuses transmission beams directly at the intended receiver while reducing the overall interference generated by the transmitter.

NOTE: Only available on 8.11+ Wireless Controllers for AP37xx, W78xC, AP38xx (Radio 2), and AP3801 (Radio 2) APs.

Enhanced Rate Control

Minimum Basic Rate
For each radio, click the minimum data rate that must be supported by all stations in a BSS. If necessary, the Max Basic Rate choices adjust automatically to be higher or equal to the Min Basic Rate.

Maximum Basic Rate
For each radio, click the maximum data rate that must be supported by all stations in a BSS.

Maximum Operational Rate
For each radio, click the maximum data rate that clients can operate at while associated with the AP. If necessary, the Max Operational Rate choices adjust automatically to be higher or equal to the Max Basic Rate.

No. of Retries

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).

Cloning an Existing AP Profile

To launch the Clone AP Profile wizard:

1. Click the Templates tab.

2. In left-hand pane, click the New bar, expand Clone and select Clone AP Profile. The Clone AP Profile wizard launches.

3. In the New template name field, enter a name for the new AP Profile.

4. In the Profile Type field, select a profile type. The Default is "All".

5. In the Controller field, select a Wireless Controller. The Default is "All".

6. Select one of the following:

   - Base template on a deployed AP – This options lets you create a template by copying the settings of an AP deployed on a Wireless Controller. To more easily find the source AP to clone, the list of APs is displayed in a table with sortable, searchable, and filterable columns.

   - Base template on a deployed AP Profile, which is one of a Wireless Controller's default AP Profiles

   - Base template on an existing AP Profile template – This option lets you create a template by copying an already configured template.

7. The window that lists the selected item becomes active. Click **View Selected** button to view detailed information about the cloning source.

8. Click **Next** to view the Cloning Summary page.

9. The Cloning Summary page displays the configuration that you selected. Click **Finish** to clone the configuration or Cancel to discard it.

Configuring APs with Professionally Installed Antennas

APs with external antennas (indoor and outdoor) including the AP3710e, AP3765e, AP3767e, AP3715e, AP3805e, AP3825e, and the AP3865e should be professionally installed. The following procedure is for configuring the power levels of APs with professionally installed antennas:

1. Determine the Antenna Model. The installer must determine the antenna model and number of antenna ports for that model. The number of antenna ports can be determined from visual inspection of the antenna or from the antenna model name itself. If the antenna model name contains a:

   - T or X (for example, PRO-AO-xTxxxxx or AO-xXxxxxx), it is a triple port antenna.

   - D (for example, PRO-AO-xDxxxxx), it is a dual port antenna.

   - S (for example, PRO-AO-xSxxxxx), it is a single port antenna.

2. Configure the Radio RF Ports, by specifying for each radio port the type of antenna attached to it. If attaching a:

   - triple port antenna, all three RF ports should be configured with the same antenna type.

   - a dual port antenna, two of the radio RF ports should be configured with the same antenna type and the third (non-active port) should be configured to 'No Antenna'.

   - a single port antenna, one of the radio RF ports should be set to the correct antenna type, and the other non-active ports should be set to 'No Antenna'.

3. Install a terminator on all ports where an antenna is not connected.

4. If the AP Profile has not been restricted to a particular hardware type during creation, then set the AP Properties (for more information, see AP Properties Tab).

5. If the AP Profile was created for a specific AP hardware type then this is also done from the AP Properties tab unless the AP hardware type

supports the Professional Install feature, in which case a secondary dialog called Professional Install is used to configure the attenuation per radio and the mapping of the radio RF ports with antenna types (for more information, see [AP Properties Tab - Professional Install Button](#)).

6. Configure the Radio Channel Related Properties. For each radio configure its Mode, Channel Width (20 MHz, 40 MHz or 80 MHz), and Channel Plan. By default the AP will auto-select a channel from the Channel Plan setting.

7. Configure the Radio's Max Transmit (Tx) Power. If the AP Profile has not been restricted to a particular AP hardware type, the full range of values (0-24 dBm) is allowed for Max Tx Power.

NOTE: If you are deploying to multiple AP hardware types or you don't need to fine tune the Max Tx Power setting, just leave it at its maximum, and each AP will automatically adjust it to its maximum allowed value.

- Based on the configured radio mode, channel plan and channel width for the specific antenna, the Professional Installer must look up the allowed Max Transit (Tx) Power setting from the FCC/IC Power Setting Tables published in the IdentiFi Wireless AP Installation Guide.

- Since Wireless Manager only lets you configure APs to use Auto Channel Selection (ACS), you must use the power setting from the 'Auto Select' row in the power settings table. This is also true if the Channel Plan includes DFS channels since when the AP operates on DFS channels, it may trigger ACS if Radar interference is detected.

- If there are additional losses (cable, attenuator) after the Radio RF port, increase the power from the table by the amount of the loss before entering the value into Max Tx Power.

- If the user chooses to restrict the AP hardware type to which the AP Profile can be applied:

  Wireless Manager automatically restricts the range of values allowed for Max Tx Power based on the country, AP hardware type, channel plan, antenna selection, antenna model, AP environment, radio mode, and channel width. No longer does the installer have to find the correct power setting from the AP's power table.

For APs that support the Professional Install feature, the range for Max Tx Power will be increased by the cable attenuation.

Max Tx Power Calculations

- Min Value is determined based on the number of chains per antennas configured; 5, 3, or 0 dBm for 3, 2 or 1 antenna respectively

- Max Value is determined based on the equation:

  Per_Chain_Power_Max [dBm] = min (Target Power, Compliance Power + Attenuation)

  Total_Power_Max [dBm] = Per_Chain_Power_Max + N chains (0, 3, 5); where N=1, 2, 3

  Attenuation [dBm] = Attenuation configured by the installer. Applies only to professionally installed APs.

  Target Power [dBm] = Specific AP Target Power set in EEPROM.

  Compliance Power [dBm] = From the official compliance tables; based on the configured country, antenna type, environment, and channel.

Viewing Summary Information About All AP Profiles

You can view summary information about AP configurations currently defined in Wireless Manager by accessing the AP Profile Summary page. From this page, you can also perform the following tasks:

- Edit, clone, or delete an existing AP profiles definition.
- Create tasks that deploy AP Profiles to APs, AP Groups, AP Load Groups and Wireless Controllers.
- Export an AP Profile configuration to the CLI.
- Create new AP Profile definition.

To view information about configured AP Profiles:

1. Click the Templates tab

2. In left-hand pane, click Access Points. The AP Profile Summary page displays.

The following list describes the information available on the Access Point Profile
Summary page.

Status

Status of the Access Point. Options include:

⭕Deployed, ⚪ Not Deployed, 🚫Deployed but not synchronized to the
network,

🟠Deployed but some templates are not synchronized

Name

Name of the Access Point. This name can be the same as the AP template
name, or it can be a different name.

Hardware Type

Information on the type of AP.

Role

Displays the role of the AP.

Radios (radio protocol)

Displays protocol information for each radio.

Controllers

Displays the IP address of the Wireless Controller.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Related Information

- [Deleting Templates](#)
- [Editing Templates](#)
- [Viewing Detailed Template Information](#)

About Classes of Service Templates in Extreme Management Center (Legacy)

A 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 policy is permitted. A standard CoS contains the following attributes:

- Marking - modifies the L2 802.1p and/or L3 ToS based on CoS definition.
- Rate limiting - inbound and outbound rate profiles.
- Transmit Queue assignment - including Transmit Queues 0-7.

This Help topic includes the following information:

- Creating a Class of Service Template
- Using Policy Manager to Create Class of Service Templates
- Viewing CoS Summary Information
- Viewing Detail Information About a CoS
- Viewing Predefined CoS Information
- Viewing Detail Information About a Predefined CoS
- Viewing Legacy CoS Information
- Viewing Detail Information About a Legacy CoS

Creating a Class of Service Template

Wireless Manager no longer supports the configuration of CoS templates. For more information, see the Legacy Template Migration Notice.

Using Policy Manager to Create Class of Service Templates

If you are using Policy Manager (PM), after you save the configuration for a particular domain which includes Wireless Controllers, Wireless Manager will automatically create for you those CoS defined in the domain. Since a CoS in Policy Manager can have different definitions in different domains, in Wireless

Manager the Navigation Tree shows a single CoS, which when clicked displays a separate tab for each domain specific version of the CoS.

CoS created on behalf of Policy Manager are located under the Templates tab > Classes of Service > Classes of Service folder.

- **Classes of Service > Predefined** contains those CoS which are predefined on both Policy Manager (except for No CoS) and on 8.01+ Wireless Controllers.

  - The No CoS - CoS means that the traffic to which it is assigned will not be remarked, subject to any rate limits, or have its default transmit queue affected. This CoS cannot be deleted or modified.

  - As for the other eight CoS, they are each associated with one of the 802.1p priorities (0-7). Although WM will allow you to modify some of their settings, you cannot change their following properties: Name, 802.1p Priority, or Use Legacy Priority Override defined in the WLAN Service. Any changes to these CoS will only be deployed to non-PM managed Wireless Controllers. Nevertheless, you can still reference these CoS in WLAN Service Templates and deploy them to PM managed Wireless Controllers, but the definitions of these CoS are assumed to have been enforced by Policy Manager to the target Wireless Controllers.

  NOTE: After migrating legacy templates these legacy predefined CoS should have been deleted and replaced by their Policy Manager counterparts: Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, RTP/Voice/Video, and High Priority. Unlike their predecessors, they appear directly under the Classes of Service tree node, they cannot be edited, and their definition is completely determined by Policy Manager.

- **Classes of Service > Legacy** contains CoS created using Wireless Manager, either manually or by cloning an existing CoS Template or deployed CoS.

Classes of Service cannot be edited with Wireless Manager.

Classes of Service cannot be deleted by the user. A PM-CoS will be automatically deleted from Wireless Manager when it is either deleted from all those domains (with assigned Wireless Controllers) were it is defined, or all the Wireless Controllers are removed from those domains were it is defined. If a PM-CoS exists in multiple domains, and instead the CoS is deleted from just one domain (with assigned Wireless Controllers) were it is defined, or all the Wireless Controllers are removed from that domain, then the corresponding domain specific version of that CoS is deleted from Wireless Manager.

Classes of Service are not deployable by themselves, but can be referenced in the deployment of a WLAN Service Template. During the deployment of a WLAN Service template referencing a PM-CoS, the user can now select the option 'Enforce using Policy Manager' to have Wireless Manager trigger Policy Manager to enforce the domain configuration on any target controllers referenced by the deployment task. If this option is not selected, Wireless Manager will assume that the PM-CoS already exists on the target Wireless Controllers. In general this is a valid assumption since the user, most likely, has already used Policy Manager to "Enforce Role Set" for the domain where these Wireless Controllers reside. In the unlikely scenario the PM-CoS doesn't yet exist on the target Wireless Controllers, Wireless Manager will fail the deployment with a suitable error message, and you can correct the problem from Wireless Manager by selecting the option 'Enforce using Policy Manager' during deployment or from Policy Manager using "Enforce Role Set".

Classes of Service don't have any Status. PM-CoS are not audited by Wireless Manager. Instead, Policy Manager detects and reports any discrepancies between CoS defined in a domain, and those CoS defined on the Wireless Controllers in the domain. Wireless Manager however will audit that a WLAN Service Template is referencing the correct PM-CoS on any target Wireless Controllers.

Classes of Service can be easily identified in drop down lists (for example, for selection in a WLAN) since their names include the name of the Policy Manager domains in which they are defined.

For information on how to create a CoS in Policy Manager, refer to the NetSight Policy Manager User Guide.

Viewing CoS Summary Information

You can view summary information about Policy Manager (PM) CoS templates currently defined in Wireless Manager from the Summary for PM-CoS page. From this page, you can see at a glance the set of Policy Manager domains where a particular PM-CoS is defined.

To view summary information for PM-CoS:

1. Click the Templates tab.

2. In left-hand pane, click Classes of Service. Expand the Classes of Service folder. The Summary for PM - CoS Page displays. This page displays the different Class of Services and the Policy domains for each specific CoS.
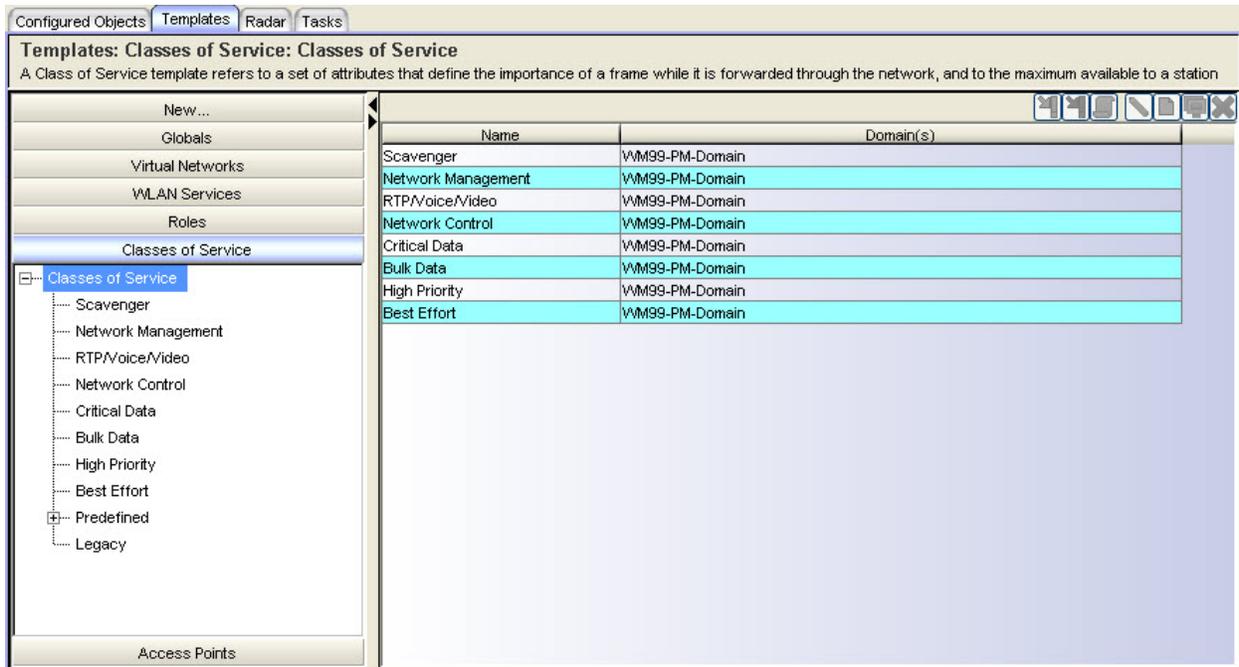
By default, Wireless Manager has several predefined CoS Templates:

- No CoS – for traffic traveling to or from the station to which this CoS is assigned, the Wireless Controller software will determine the appropriate transmit queue, will not impose any rate limits, and will not re-mark its priority. This CoS cannot be edited or deleted.

- Wireless Manager also supports the following predefined CoS Templates (defined in Policy Manager) listed in order of increasing 802.1p priority: Scavenger, Best Effort, Bulk Data, Critical Data, Network Control, Network Management, RTP/Voice/Video, and High Priority. These CoS templates cannot be deleted, and their 802.1p setting cannot be edited.

NOTE: After migrating legacy templates, these legacy predefined CoS should have been deleted and replaced by their Policy Manager counterparts. Unlike their predecessors, they appear directly under the Classes of Service tree node, they cannot be edited, and their definition is completely determined by Policy Manager.

Viewing Detail Information About a CoS

To view information about a configured CoS:

1. Click the Templates tab

2. In left-hand pane, click Classes of Service, and expand the Classes of Service folder and select a CoS. The CoS Details page displays.
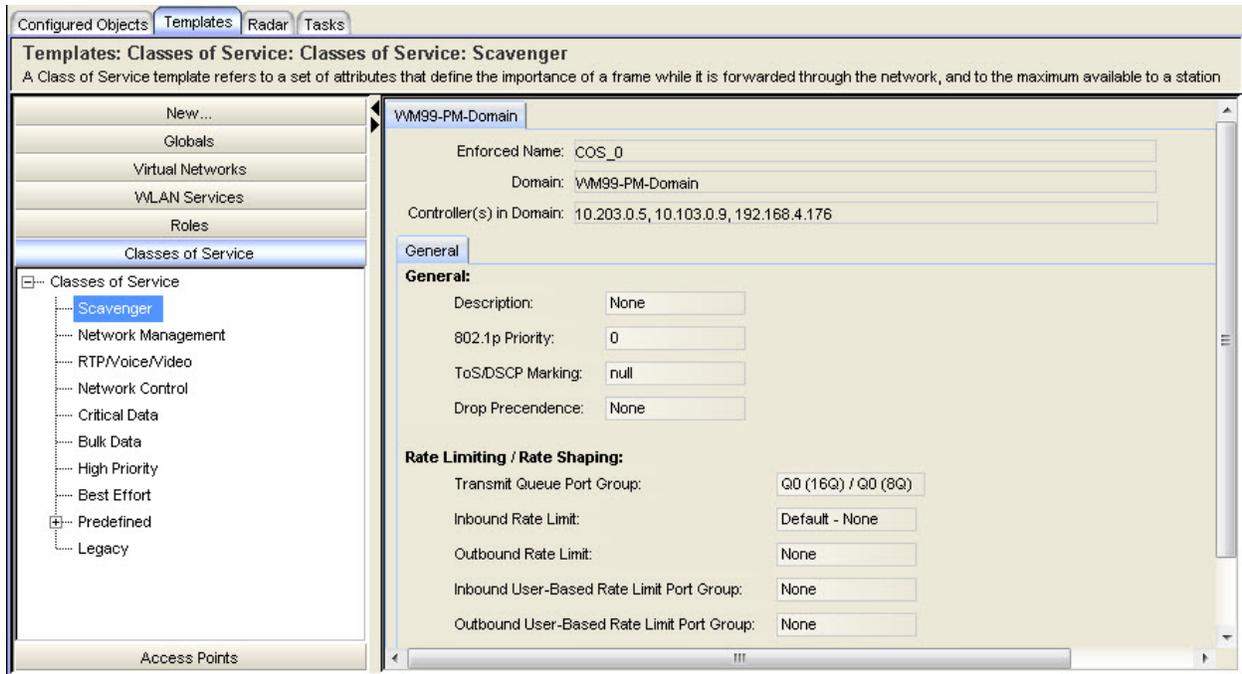
NOTE: Policy Manager CoS can have different definitions in different domains.

The following list describes the information available on the CoS Details page.

Enforced Name
Name of this CoS if it were deployed to a Wireless Controller in that domain.

Domain
Domain name.

Controller(s) in Domain
IP addresses of all controllers assigned to the specified Policy Manager domain.

General Tab
Please refer to the *Policy Manager User Guide* for details.

Viewing Predefined CoS Information

Wireless Manager no longer supports the configuration of CoS templates. For more information, see the Legacy Template Migration Notice. You can view

summary information about the Predefined CoS in Wireless Manager from the Summary for Predefined CoS page.

To view summary information for a Predefined CoS:

1. Click the Templates tab.

2. In left-hand pane, click Classes of Service > Predefined. The Summary for Predefined CoS Page displays.

The following list describes the information available on the Predefined CoS page.

Status

Status of this CoS. The possible status values are:

Not deployed, Deployed, Deployed but not synchronized to the network,

Deployed but some child templates are not synchronized.

Name

Name assigned to the CoS.

Type

Displays the CoS type.

802.1p

Displays the Layer 2 priority (Priority 0 to 7).

ToS/DSCP

Displays the ToS/DSCP marking.

Inbound Rate Profile

Displays the inbound rate limit.

Outbound Rate Profile

Displays the outbound rate limit.

TXQ

Displays the TXQ override.

Controllers

Wireless Controller to which this CoS has been deployed.

Toolbar Buttons

For a description of common toolbar buttons see <u>Context-Sensitive Toolbar</u>.

Viewing Detail Information About a Predefined CoS

To view information about a Predefined CoS:

1. Click the Templates tab.

2. In left-hand pane, click Classes of Service. Expand the Predefined folder and select a Predefined CoS. The Predefined CoS Details page displays with the Template Properties tab active. For more information about the fields on this tab, see the <u>Template Properties Tab</u> Help topic.

3. Click on the Class of Service Properties tab to view read-only properties for the CoS.

Viewing Legacy CoS Information

Wireless Manager no longer supports the configuration of CoS templates. For more information, see the Legacy Template Migration Notice. You can view summary information about Legacy CoS templates currently defined in Wireless Manager from the Summary for Legacy CoS page.

To view summary information about configured Legacy CoS:

1. Click the Templates tab.

2. In left-hand pane, click Classes of Service, and expand the Classes of Service folder and click Legacy. The Summary for Legacy CoS page displays.

The following list describes the information available on the Classes of Services page.

Status

Status of this CoS. The possible status values are:

⊙ Not deployed, ⊙ Deployed, ⊗ Deployed but not synchronized to the network,

⊗ Deployed but some child templates are not synchronized.

Name

Name assigned to the CoS.

Type

Displays the CoS type.

802.1p

Displays the Layer 2 priority (Priority 0 to 7).

ToS/DSCP

Displays the ToS/DSCP marking.

Inbound Rate Profile

Displays the inbound rate limit.

Outbound Rate Profile

Displays the outbound rate limit.

TXQ

Displays the TXQ override.

Controllers

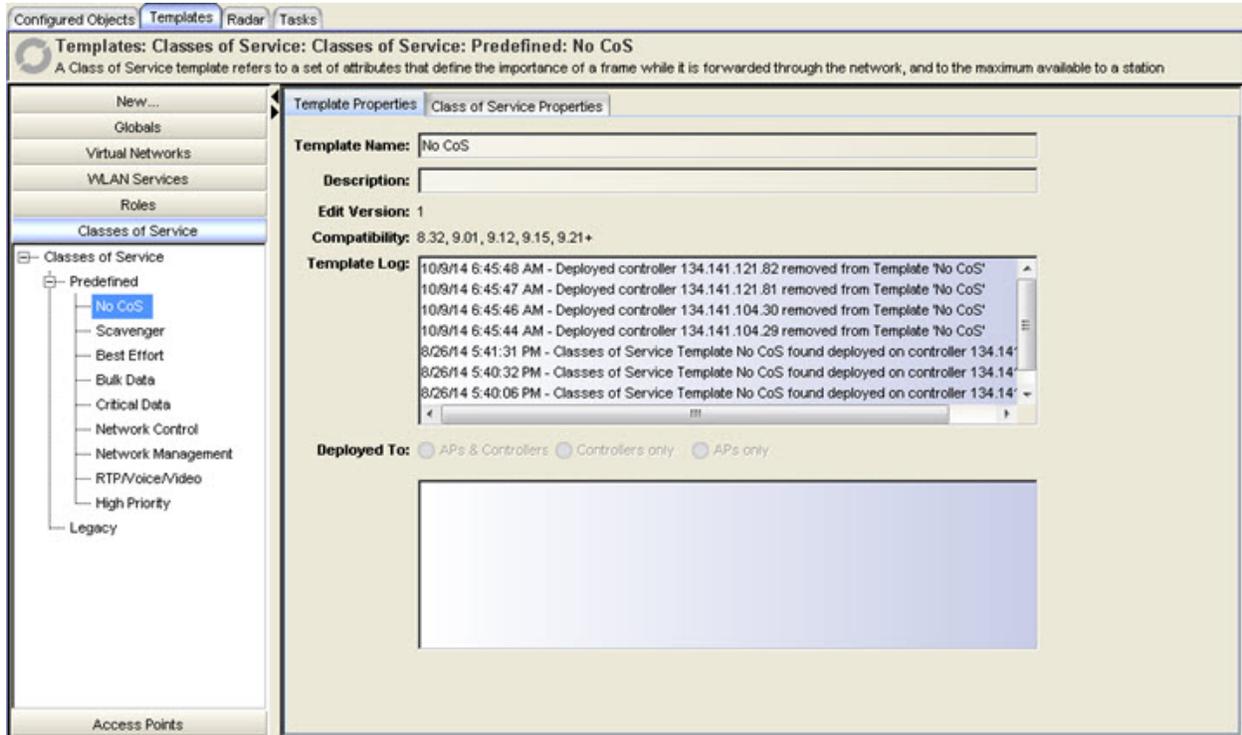Wireless Controller to which this CoS has been deployed.

Viewing Detail Information About a Legacy CoS

Wireless Manager no longer supports the configuration of CoS templates. For more information, see the Legacy Template Migration Notice. To view detail information about a Legacy CoS:

1. Click the Templates tab.

2. In left-hand pane, click Classes of Service. Expand the Classes of Service folder. Expand the Legacy folder and select a Legacy CoS. The Legacy CoS Details page displays with the Template Properties tab active. For more information about the fields on this tab, see the Template Properties Tab Help topic.
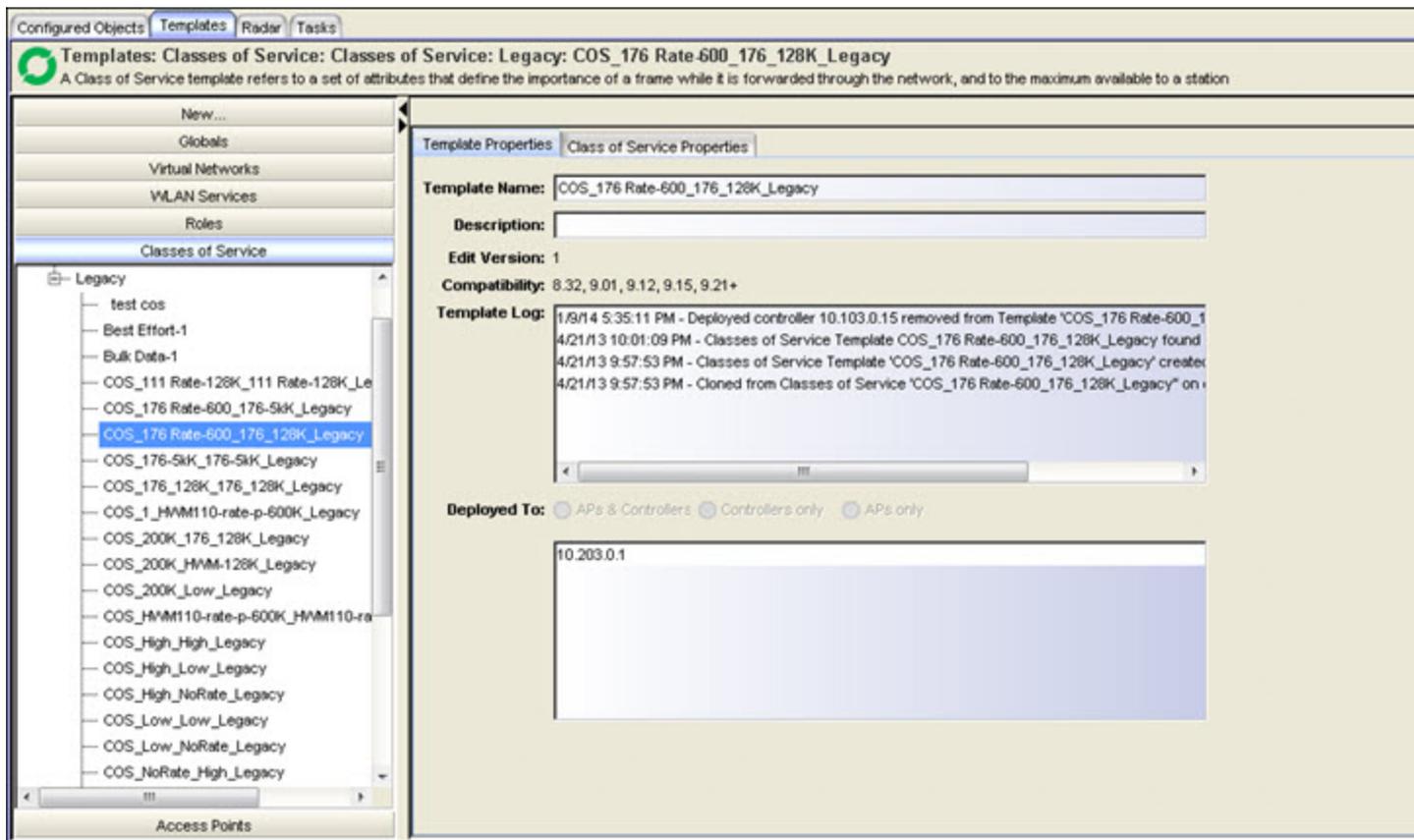
Class of Service Properties Tab

Core

Name
The name by which this CoS will be known by on the Wireless Controller.

Marking

Use Legacy Priority Override defined in the WLAN Service
Select this checkbox to use the Priority Override defined in the WLAN as in previous releases.

Rate Limiting

Inbound Rate Limit
Select this checkbox, and then select an inbound rate limit from the drop-down list.

Outbound Rate Limit
Select this checkbox, and then select an outbound rate limit from the drop-down list.

Transmit Queue Assignment

Transmit Queue
Select this checkbox, and then 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.

About Radar in Extreme Management Center (Legacy)

Radar is a set of advanced, intelligent, Wireless-Intrusion-Detection-Service-Wireless-Intrusion-Prevention-Service (WIDS-WIPS) features that are configurable from Wireless Manager. 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.

The ExtremeWireless Wireless Controller supports three kinds of scan profiles: Out-of-Service, In-Service, and Guardian.

NOTE: Out-of-Service scan profiles only apply to AP26xx and AP36xx and are not supported by Wireless Manager.

When Radar is enabled, the 37xx and 38xx APs will:

- Simultaneously provide WIDS-WIPS and wireless bridging functions.
- If configured to do so, take active countermeasures against specific types of threat that they have detected (for more information, see Prevention Tab).

NOTE: The 3705 type APs will only monitor and protect the channels for which they are bridging traffic.

This Help topic includes the following information:

- In-Service Scan Profiles
- Guardian Scan Profiles
- Cloning an Existing Radar Profile
- Radar Maintenance
- Security Threats
- Preventive Measures

In-Service Scan Profiles

In-Service scan profiles work with APs based on the 37xx, and 38xx architecture and include the following:

- Whether to scan for security threats (Ad Hoc, Cracking, DoS, Internal / External Honeypot, Performance, Prohibited Device, Spoofed AP, Surveillance) and / or to classify sources of interference (Radar, Microwave, Phone, Video Bridge, Bluetooth Stereo, Bluetooth Headset, CWA).

- A set of countermeasures that lists possible prevention options to counter specific types of threats. Includes the ability to automatically blacklist clients originating DoS / password cracking attacks. If blacklisting clients is enabled, you can set the maximum amount of time a device can be blacklisted (for more information, see Prevention Tab).

NOTE: 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 Out-of-Service scan profiles will be retained. However, the Out-of-Service 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.

In Wireless Manager, APs are not part of the scan profile template definition, but are assigned during template deployment. Since only APs local to a given controller can be selected, if you want to assign foreign APs to your scan profile you must manage both controllers in an availability pair. Moreover, if you want to deploy your scan profile to an AP that is already assigned to another scan profile, it must first be removed from its current scan profile.

Viewing Summary Information About In-Service Scan Profiles

To view information about In-Service scan profiles configured in Wireless Manager:

1. From the top menu, click Radar.

2. In the left pane, click Scan Profiles. The Scan Profiles summary page displays.

The following list describes the information available on the In-Service Scan Profile Summary page.

Status

Status of the scan profile. The possible status values are:
 Deployed, Not deployed, Deployed but not synchronized to the network.

Name

The name of the scan profile.

Security Scan

Indicates whether the profile enables security scanning on APs assigned to this profile.

Classify Interference

Indicates whether the classification of sources of interference have been enabled for this profile.

Controllers

IP address of the controller(s) to which this scan profile has been deployed.

Toolbar Buttons

For a description of common toolbar buttons see Context-Sensitive Toolbar.

Creating an In-Service Scan Profile

You can create an In-Service scan profile template either manually, or by cloning an existing or deployed template.

Manually Creating an In-Service Scan Profile

To manually create an In-Service template:

1. From the top menu, click Radar

2. In the left pane, click Scan Profiles. The Scan Profiles summary page displays.

3. Click the New icon ⬚. A blank Template Properties tab displays.
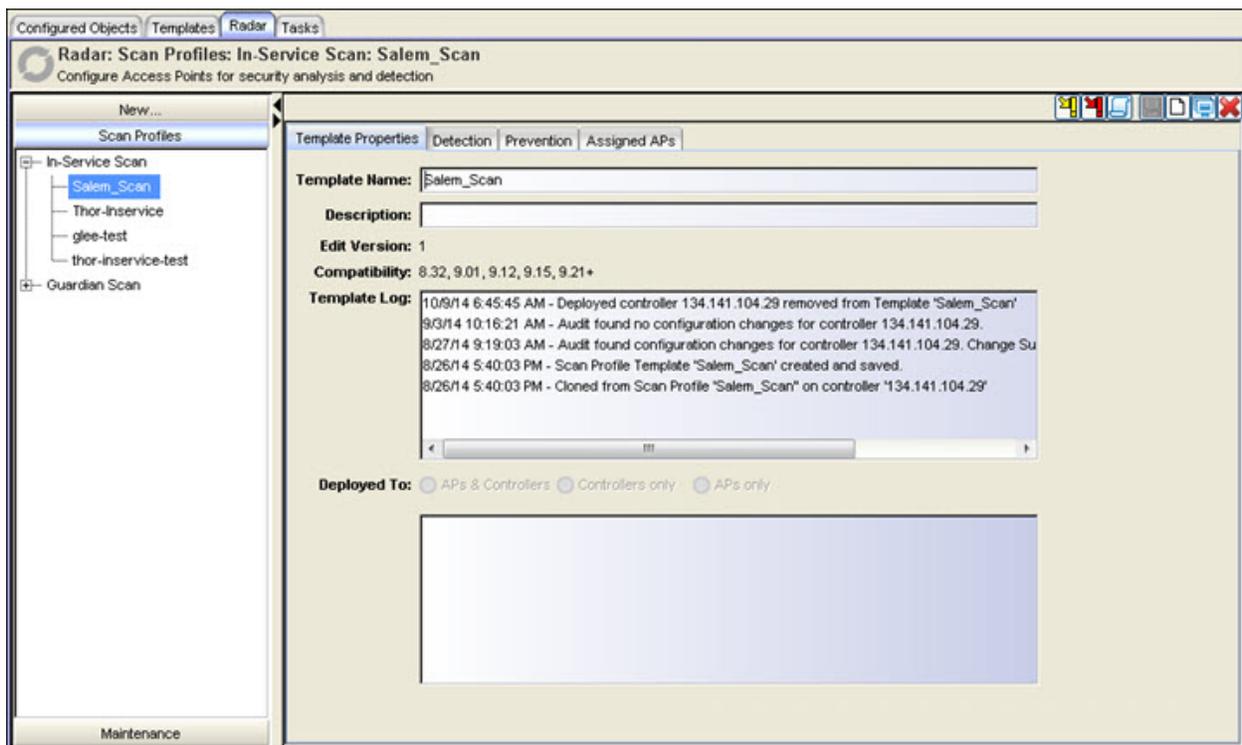
4. Enter a name for the new template. Enter a template description, if desired. For more information about the fields on this tab, see the [Template Properties Tab](#) Help topic.

The following list describes the information available in the tabs on the In-Service Scan Profiles Details page.

Detection tab

Core

Name

Type a unique name for this scan profile.

Scan for security threats

Select to scan for security threats (for more information, see <u>Security Threats</u>).

Rogue AP Detection

Select this option to detect rogue APs serving open SSIDs (for example, an AP attached to an Ethernet wall jack and the AP is running an open SSID). If a rogue AP is detected, countermeasures can be optionally applied to prevent any station from using this rogue AP.

Listener Port

Enter the UDP port for rogue AP detection.

Classify Source 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 37xx, and 38xx architecture are capable of performing interference classification

Prevention Tab

Countermeasures

Select the appropriate prevention measures for the selected profile. For a description of each option, see <u>Preventive Measures</u>.

Assigned APs Tab

Shows the list of APs by controller to which this scan profile template as been deployed.

Guardian Scan Profiles

Guardian scan profiles are only supported by the AP3710(i/e), AP3715(i/e), AP3765(i/e), AP3767e, AP3805(i/e), AP3825(i/e), and AP3865e. APs assigned to a Guardian scan profile operate in a dedicated Radar mode.

- An AP operating in Guardian mode does not bridge traffic and instead devotes all of the AP's resources to threat detection and countermeasures.

- An AP is added to a Guardian scan mode in its entirety. There is no option to dedicate one radio to scanning and the other to forwarding.

- An AP assigned to a Guardian scan profile stops providing any services (WLAN service, load groups, site) immediately.

Guardians don't count towards the number of APs licensed by NetSight. APs servicing a WDS / mesh WLAN cannot be added to a Guardian scan profile.

When an AP is added to a Guardian scan profile it retains its AP, radio and WLAN service settings, which you can continue to configure (using AP Profile templates) like those of any other AP. Some settings, such as changes to antenna and country, are even forwarded to Guardians.

Unlike APs assigned to in-service scan profiles which only monitor and protect the channels for which they are bridging traffic, APs assigned to guardian scan profiles will monitor and protect those channels specified in the template. A guardian however will not perform active countermeasures or scan regulatory prohibited channels, nor will it defend against threats on DFS channels but will perform passive scanning of DFS channels in order to detect and report such threats.

Viewing Summary Information About Guardian Scan Profiles

To view information about Guardian scan profiles configured in Wireless Manager:

1. From the top menu, click Radar.

2. In the left pane, click Scan Profiles > Guardian Scan. The Guardian Scan Profiles summary page displays.

The following list describes the information available on the Guardian Scan Profile Summary page.

Status

Status of the scan profile. The possible status values are: 🟢 Deployed, ⚪ Not deployed, 🛑 Deployed but not synchronized to the network.

Name

The name of the scan profile.

Security Scan

Indicates whether the profile enables security scanning on APs assigned to this profile.

Classify Interference

Indicates whether the classification of sources of interference have been enabled for this profile.

Controllers

IP address of the controller(s) to which this scan profile has been deployed.

Toolbar Buttons

For a description of common toolbar buttons see Context-Sensitive Toolbar.

Creating a Guardian Scan Profile

You can create a Guardian scan profile template either manually, or by cloning an existing or deployed template.

Manually Creating a Guardian Scan Profile

To manually create a Guardian template:

1. From the top menu, click Radar

2. In the left pane, click Scan Profiles. The Scan Profiles summary page displays.

3. Click the Guardian Scan tree node.

4. Click the New icon ⬜. A blank Template Properties tab displays.
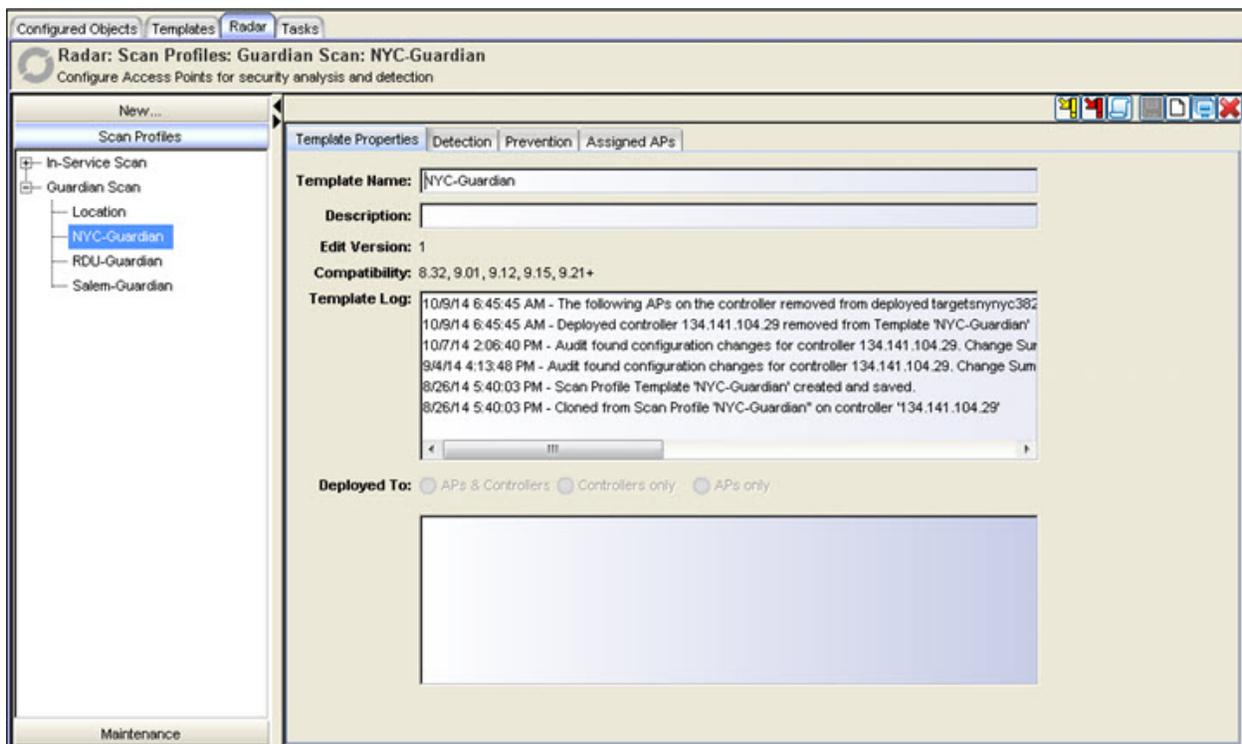
5. Enter a name for the new template. Enter a template description, if desired. For more information about the fields on this tab, see the [Template Properties Tab](#) Help topic.

The following list describes the information available on the Guardian Scan Profiles Details page.

Detection Tab

Core

Name
Type a unique name for this scan profile.

Scan for security threats
Select to scan for security threats (for more information, see Security Threats).

Classify Source 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 37xx architecture are capable of performing interference classification.

Channels to Monitor

2.4 GHz
Click the 2.4 GHz tab and select additional channels to be monitored within this band for the scan profile.

5.0 GHz
Click the 5 GHz tab and select additional channels to be monitored within this band for the scan profile.
Note: The AP371x and AP38xx automatically scan 40 MHz and 20 MHz wide channels.

Prevention Tab

Countermeasures
Select the appropriate prevention measures for the selected profile. For a description of each option, see Preventive Measures.

Defense Options
Select the maximum number of channels to defend concurrently. This option applies separately to each radio of a Guardian AP so that overall it can defend concurrently a maximum of 8 channels but only 4 on each radio.

Assigned APs Tab

Shows the list of APs by controller to which this scan profile template as been deployed.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

Cloning an Existing Radar Profile

To launch the Clone Scan Profile wizard:

1. Click the Radar tab.

2. In left-hand pane, click the New bar, expand Clone and select:

   - Clone an In-Service Scan Profile, the Clone Scan Profile Wizard launches

   - Clone a Guardian Scan, the Clone Scan Profile Wizard launches

   - Clone Radar Maintenance, the Clone Radar Maintenance Wizard launches

3. In the New template name field, enter a name for the new template.

4. Select one of the following:

   - Base template on a deployed Scan Profile Template – This options lets you create a template by copying the settings of a deployed template on a Wireless Controller.

   - Base template on an existing Scan Profile Template – This option lets you create a template by copying a template that is already configured.

5. The window that lists the selected item becomes active. Click the View Selected button to view detailed information about the cloning source. Click **Next** to view the Cloning Summary page.

6. The Cloning Summary page displays the configuration that you selected. Click **Finish** to clone the configuration or **Cancel** to discard it.

Radar Maintenance

The Radar Maintenance template is used to maintain the Radar lists of APs. You can view summary information about Radar Maintenance templates currently defined in Wireless Manager from the Radar Maintenance Summary page. From this page, you can also perform the following tasks:

- Deploy the template.

- Edit, clone, or delete an existing Radar Maintenance template.

- Export a Radar Template configuration to the CLI.

- Create new Radar Maintenance templates.

To view summary information about configured Radar Maintenance templates:

1. Click the Radar tab.

2. In left-hand pane, click Maintenance. The Radar Maintenance Summary page displays.
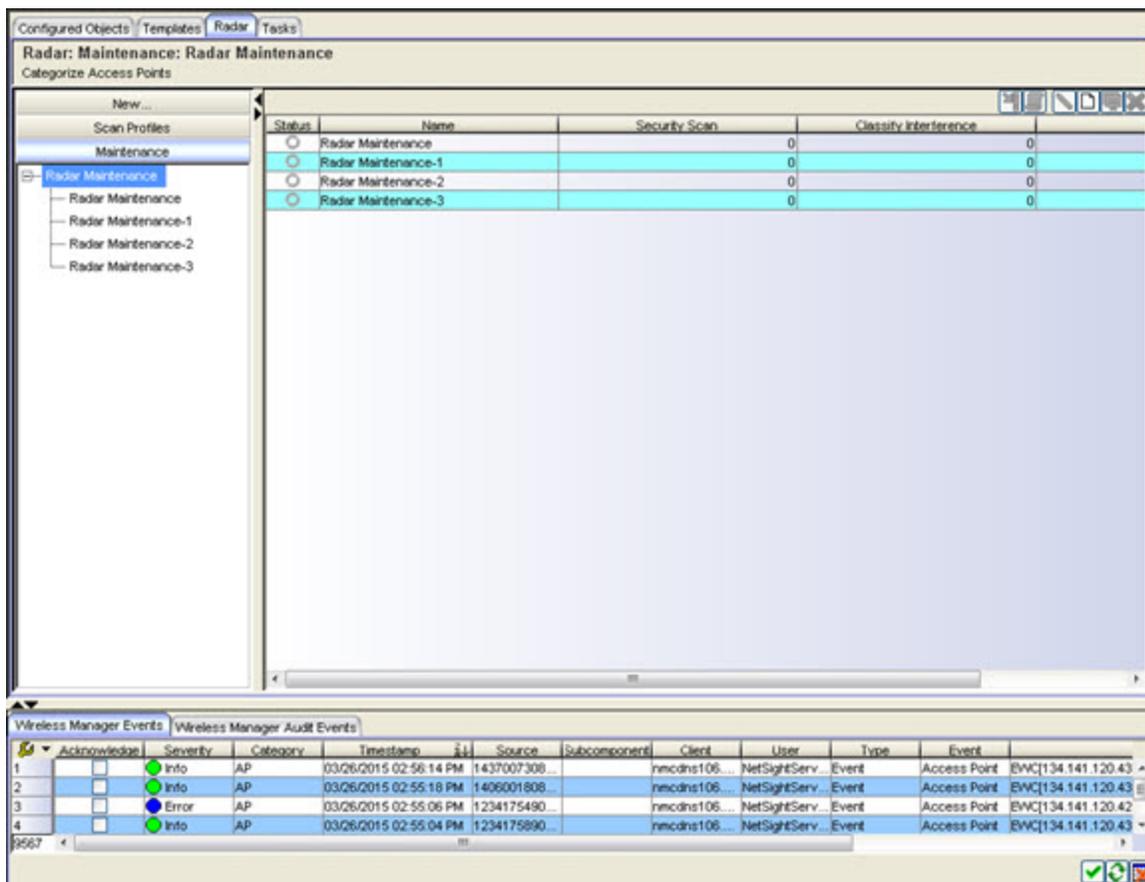
The following list describes the information available on the Radar Maintenance Summary page.

Status

Status of this Radar Maintenance template. Options include:

⊙ Deployed, ○ Not Deployed, ⊘ Deployed but not synchronized to the network,

⊘ Deployed but some templates not synchronized.

Name

Name assigned to the Radar Maintenance template.

Security Scan

Indicates whether the profile enables security scanning on APs assigned to this profile.

Classify Interference

Indicates whether the classification of sources of interference have been enabled for this profile.

Controllers

IP address of the controller(s) to which this scan profile has been deployed.

Toolbar Buttons

For a description of common toolbar buttons see [Context-Sensitive Toolbar](#).

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.

Radar Maintenance templates can be deployed to 8.21+ Wireless Controllers (EWC) with Security Analysis Engine enabled. When creating a Radar Maintenance template, it is recommended to select all Wireless Controllers from the same mobility zone. When a new template is created, the "Load Scan Results" button retrieves all Authorized, Friendly, Prohibited, and Uncategorized APs from the selected controllers. For an existing template, its label changes to "Load Uncategorized APs" and it only retrieves Uncategorized APs from selected controllers. If an AP is found in multiple categories, any conflicts are resolved according to the following priority: Prohibited > Authorized > Friendly > Uncategorized

AP Categories

APs are labeled as belonging to one of the following categories when they are added to the Analysis Engine database:

- Uncategorized APs - Scanned APs that do not fall into any other category.

- 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.

- 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. This is useful if 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. WM has the added convenience of being able to add all those APs from any managed controller. Note: The set of Authorized APs deployed to each EWC will only include those APs which are considered Pre-Authorized on that EWC. Any "hidden" Authorized APs (i.e., those local & foreign APs associated with the EWC) will be excluded, for the purpose of deployment and auditing.

  Pre-Authorized = Authorized APs of template – local APs of the target EWC and peer.

- Prohibited APs - APs 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 those that were stolen from the authorized network and now could be used to generate a security breach.

  When a prohibited AP is detected, the following actions can be taken:

  - Report presence only - When the MAC address of the prohibited AP is detected by an authorized scanning AP, the prohibited APs presence will be reported in an event message. This will result in the presence of the MAC being included in the Radar threat reports. Radar will not take any countermeasures against the device with the MAC address.

  - 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.

Differences between the Radar Maintenance Template and Other Templates:

- Import Behavior: Unlike other templates, when importing Radar Maintenance settings, a template is not matched based on is content, but instead by its selected controllers. If a template exists for the EWC, the imported Uncategorized, Friendly, Authorized, and Prohibited APs will be merged with those of the existing template. Any conflicts are resolved by leaving the AP in its current category. If no template exists for the EWC a new template is created.

- Audit: Authorized, Friendly, and Prohibited APs are audited. Uncategorized APs are not audited.

- Undeploy: If a controller is unselected during deployment, the Radar Maintenance settings on that EWC are not changed.

Manually Creating Radar Maintenance Template

To manually create a Radar Maintenance template:

1. From the top menu, click Radar

2. In the left pane, click New > Add Radar Maintenance. A blank Template Properties tab displays.
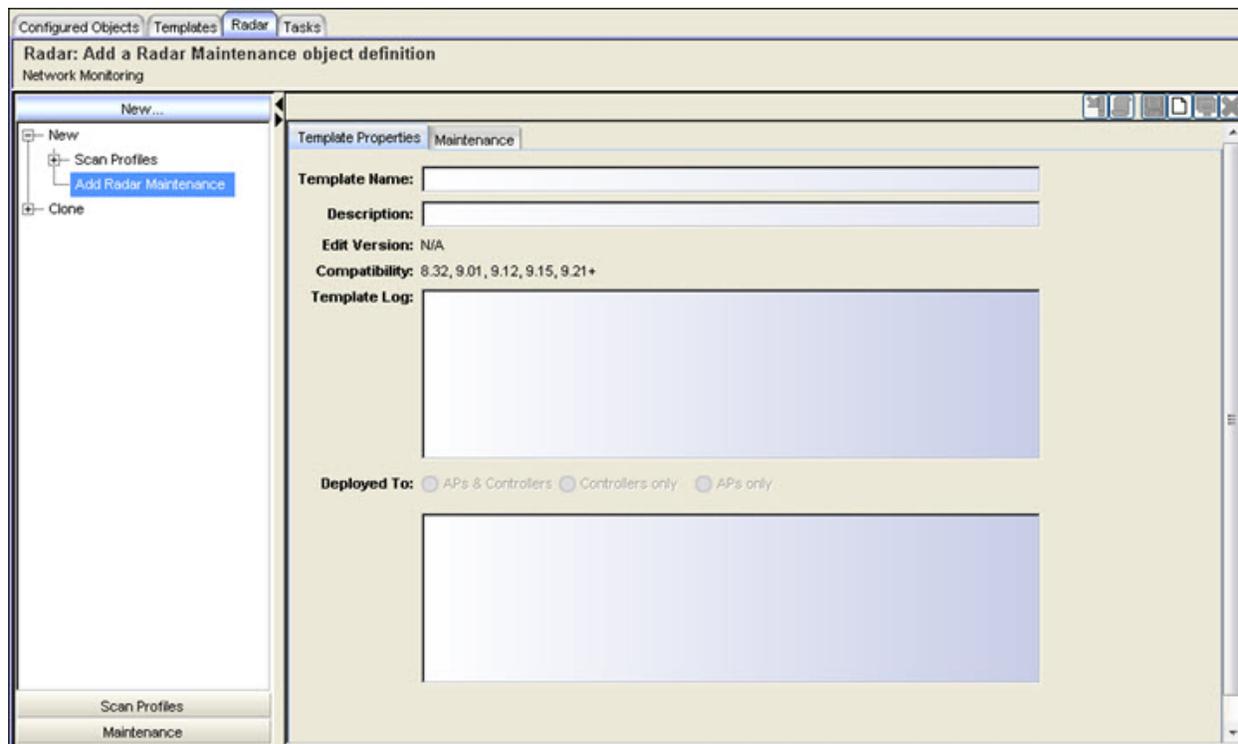
3. Enter a name for the new template. Enter a template description, if desired. For more information about the fields on this tab, see the Template Properties Tab Help topic.

The following list describes the information available on the Radar Maintenance Profiles Details page.

Maintenance Tab

Selected Controllers
List of 8.21+ managed Wireless Controllers with Security Analysis Engine enabled.

Access Points
Displays the lists of APs by category. Categories include: Uncategorized, Friendly, Authorized, and Prohibited.

Assign APs
Select a new category for the selected AP (from the category tabs under Access Points) and click Apply.

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 Wireless Manager, the controller's GUI, or CLI. By default the location attribute is empty for all APs, which implicitly corresponds to a location of "World". 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 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.
- **Cracking** - This refers to attempts to actively 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 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.
- **Performance** - Performance issues pertain to overload conditions that cause a service impact. Performance issues aren't necessarily security threats, 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.
- **Rogue AP** - An unauthorized AP connected to the authorized wired or wireless network. Any type of threat can be further classified as a 'Rogue'.

In addition, uncategorized and friendly APs that are found to be connected to the authorized network can be classified as rogue threats.

- **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.

Rogue/Threat/Interference - Active & Inactive/Aged Events

Wireless Manager receives threat and interference events from 8.21+ Wireless Controllers and forwards them to Console which triggers alarms on APs, clients, and controllers to be automatically created and cleared. As for the "Rogue AP" events reported by 8.01 & 8.11 Wireless Controllers, Wireless Manager converts them to threats and handles them in the same way as threats reported by 8.21+ Wireless Controllers.

NOTE: After the release of 9.01 Wireless Controllers, the term 'Rogue' is used to identify those threats that have been determined to be connected to the authorized network.

Threats and interference events are uniquely identified by the following attributes:

- **Threat Name** - All threats have a well defined name. Interference events have the following names: Radar, Microwave, Phone, Video Bridge, Bluetooth Stereo, Bluetooth Headset, and CWA.

- **Subject MAC** - The MAC to which this threat applies. For spoofed AP, internal / external honeypot it is the advertised BSSID of the threat AP. For threats tracked at "MAC" scope, it is the address against which the threat is tracked. For all other threats this field is the broadcast MAC address (FF:FF:FF:FF:FF:FF).

- **Location** - A hierarchical string like "World/Canada/Ontario/Thornhill/...". Default is "World".

- **Channel** - The detected frequency in MHz.

Whether an AP detects a threat or source of interference on the channel that it is providing service on or as a result of scanning across multiple channels, it will send an "Active" event to the Wireless Controller when it is first detected and an "Inactive" event when it is no longer detected. Such events are forwarded to

Wireless Manager, which sends them to Console to be correlated into alarms against APs, clients, and controllers.

An "Active" alarm is automatically cleared when an "Inactive" event is received from the Wireless Controller for the same attributes as the "Active" threat (for example, threat name + subject MAC + location + channel). If for some reason the AP fails to report to the controller that a threat is no longer active, after one hour of inactivity, the Wireless Controller will automatically report the threat to Wireless Manager as "Aged".
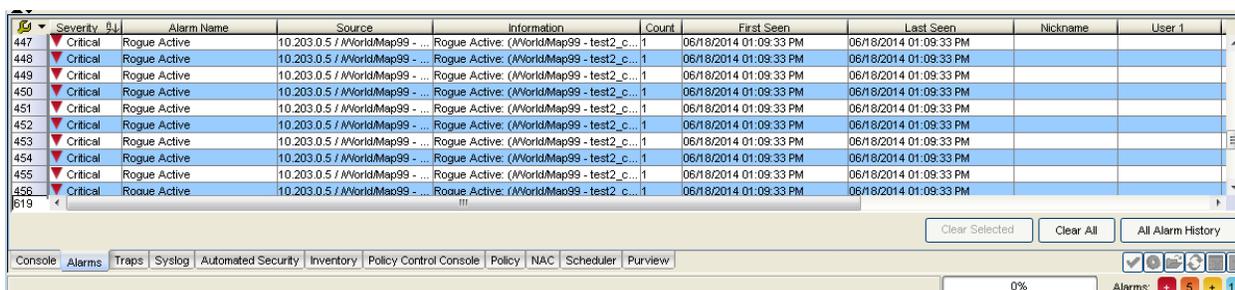
When a threat is also determined to be a 'rogue', in addition to creating the "Threat Active" alarm (with Warning severity), Wireless Manager will also create a "Rogue Active" alarm (with Critical severity).

If the controller reports that the threat is still active but no longer considered to be a rogue, Wireless Manager will clear the "Rogue Active" alarm.

If the controller reports that the threat is no longer active, Wireless Manager will create a "Threat Inactive" alarm, which will clear any "Threat Active" or "Rogue Active" alarms with the same key (threat name + subject MAC + location + channel).

To view the list of active threats (including sources of interference), click the Alarms tab located at the bottom of the NetSight screen. For more information on the Alarms Tab, see the *NetSight Console User Guide*.

Alarms Tab

Threat and interference events from Wireless Manager are correlated into alarms in Console according to the "Rogue Active", "Rogue Inactive", "Threat Active", "Threat Inactive", "Interference Started", and "Interference Stopped" alarm definitions in the Alarms Manager.

To configure the various threat related alarms, click the Alarms Manager icon located on the NetSight Toolbar. For more information on the Alarms Manager Window, see the *NetSight Console User Guide*.

Alarms Manager Window
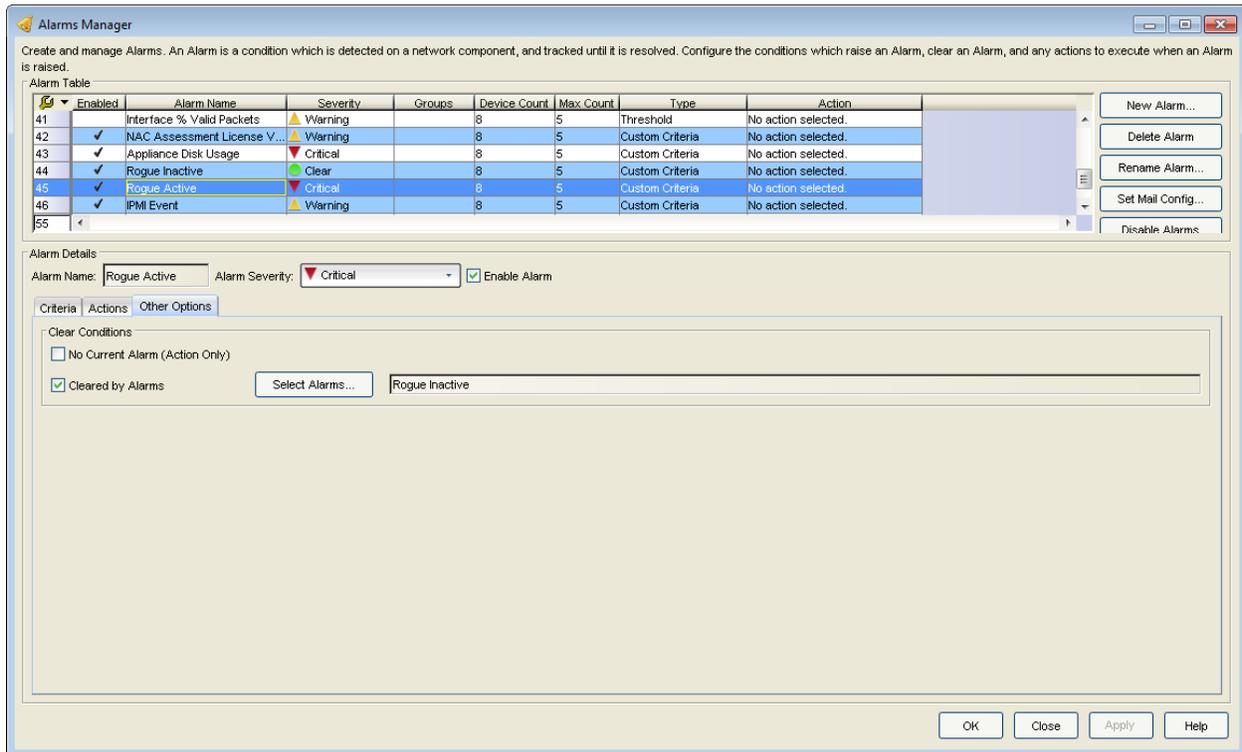
Rogue Detection and Prevention

Both Guardian and In-Service Scan Profiles can be configured to perform rogue detection and prevention. Although In-Service scan profiles support rogue detection for 9.01 or later controllers, Guardian scan profiles only support rogue detection for 9.12 or later controllers.

The ability of the controller to detect rogues, is currently limited to rogue APs serving open SSIDs. This is intended to catch the more common scenario of an employee innocently attaching an AP (running an open SSID) to his Ethernet jack.

Rogue Detection

Rogue Detection is licensed as part of any Wireless Controller Radar capacity license. The following categories of BSSIDs are excluded from the rogue detection mechanism:

- Authorized and Pre-Authorized BSSIDs
- Encrypted BSSIDs

- Spoofed APs

The Wireless Controller considers the following categories of BSSIDs as potentially rogue; they are tested in descending priority order:

- Threat
- Uncategorized
- Friendly

Rogue Testing

Rogues are re-tested after four hours (in the following order): Rogue, and then Rogue Candidates (Threat, Uncategorized, Friendly). The testing AP associates to the candidate rogue like a normal wireless client, and upon success:

- Initiates DHCP exchange to obtain an IP address.
- ARPs for the gateway MAC.
- Sends Layer 3 test messages to the wired interface of the testing AP. If the testing AP receives any of the messages then the candidate rogue is considered connected to the authorized or corporate network and its status is updated to rogue.

The testing AP reports the following information for a rogue:

- The client wireless MAC address that was inserted as the source in the L2 header.
- The source MAC address received at the wired interface. If it matches the client wireless MAC address, the rogue is on the same segment and is bridging rather than routing or NATing. If it is different, then there is a router or NAT between the AP's wireless and wired interfaces on the network. The rogue could be routing or NATing.
- The IP address issued to the client wireless interface by DHCP.
- The IP address in the source address field of the L3 header. If this differs from the IP address assigned to the AP's wireless client interface, then there is a NAT between the AP's wireless client interface and the AP's wired interface. If it is the same then there is no NAT between the AP's wireless client and wired interfaces.
  - The difference between the TTL in the frame when it was sent from the wireless client and the TTL in the frame received at the AP's wired interface.

Rogue Prevention

Once detected, a rogue AP must be isolated to prevent it from being used. APs performing countermeasures against rogue APs:

- Send de-authentication frames to its clients on behalf of the rogue AP; they are treated like spoofing APs with users being prohibited from using the rogue AP via a combination of broadcast de-authentications and targeted de-authentications.

- May have other tasks to perform limiting their ability to prevent stations from associating to the rogue for short periods of time.

Preventive Measures

This section describes the countermeasures that can be configured for In-Service and Guardian scan profiles using the Prevention tab.

- **Prevent authorized stations from roaming to external honeypot APs** - An AP that is attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport.

- **Prevent authorized stations from roaming to friendly APs** -APs that are not part of the authorized network, but operate in the vicinity of the authorized network.

- **Prevent any station from using an internal honeypot AP** - 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** - An unauthorized AP connected to the authorized wired or wireless network.

- **Prevent any station from using a spoofed AP** - An AP that is not part of the authorized network but 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 (for example, rate limiting the flooded frames)** - For preventing some types of Denial of Service (DoS) attacks from affecting the authorized network instead of just the target AP.

- **Prevent any station from using an ad-hoc mode device** - Deauthentication messages are used to prevent devices from using an ad hoc mode device.

- **Remove network access from clients originating DoS attacks and password cracking attacks** - Used to prevent the propagation of the DoS attack from the AP to the authorized network. Many types of DoS attacks 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** - Used to prevent 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.

Managing Wireless Manager Tasks (Legacy)

A task deploys or transfers a template configuration from the Wireless Manager to one or more target Wireless Controllers.

This section includes the following topics:

- [About Tasks in Extreme Management Center (Legacy)](#)
- [Creating, Scheduling, and Deploying Tasks in Extreme Management Center (Legacy)](#)
- [Deploying a Template in Extreme Management Center (Legacy)](#)
- [Deploying Point of Presence in Extreme Management Center (Legacy)](#)
- [Deploying WLAN Service Assignments in Bulk in Extreme Management Center (Legacy)](#)
- [Monitoring Tasks in Extreme Management Center (Legacy)](#)

About Tasks in Extreme Management Center (Legacy)

When you create a new or modify an existing template configuration, it is stored in Wireless Manager and does not take effect until you activate the changes. Depending on the type of template, you activate the configuration changes by creating a task that deploys the template to one or more Wireless Controllers, APs, AP Groups, or AP Load Groups.

When a task executes, Wireless Manager logs into the target Wireless Controller's CLI and deploys the template so that the Wireless Controller's configuration matches the template configuration. The task records the outcome of the execution, saves it as part of the task and logs the event.

Tasks provide progress reports when they execute. Wireless Manager displays information about the percentage of task completion as well as information about the user who initiated the task. If two tasks execute at the same time and they have conflicting requirements (for example, if each task configures the same Wireless Controller) the tasks will run serially. Wireless Manager generates an event to show which one of the tasks was delayed and why.

Upon task execution, Wireless Manager performs the following:

- Applies the template configuration to each target Wireless Controller identified by the task and updates the Wireless Controller configuration with the data specified for it in the task.

- Updates the task details page to contain a summary description of the execution process as well as the complete set of CLI scripts that executed as part of the task.

- Sets the task status to success, partial success or failure based on the outcome of task execution.

- Updates the templates on which the task was based to include a history record showing that an attempt to deploy them was made at a particular date and time and to show whether the Wireless Controller configuration is synchronized to the template.

- Updates the list of currently deployed targets.

- Generates a log to record the task executed and its success.

- Augments the task description with a history showing which objects the task was applied and whether the task succeeded on that object or not.

- Generates events for any significant task failure.

Creating, Scheduling, and Deploying Tasks in Extreme Management Center (Legacy)

The Wireless Manager provides wizards that take you through the steps of creating, scheduling, and deploying a task. During task creation you can:

- Select appropriate targets.
- Select the time at which the task will run.
- Collect customization data for each Wireless Controller.

After you have created a task, you can later suspend and reschedule the tasks as long as they have not begun to deploy.

Available task deployment wizards include:

Configured Objects Tasks

- Deploy RADIUS
- Deploy Topology

VNS Tasks

- Deploy VNS
- Deploy WLAN Service
- Deploy WLAN Assignments
- Deploy Point of Presence

Global Tasks

- Deploy Globals Template

AP Tasks

- Deploy AP Profile

Radar Tasks

- Deploy In-Service Scan Profile
- Deploy Guardian Scan Profile
- Deploy Radar Maintenance Template

Deploying a Template in Extreme Management Center (Legacy)

Creating a Task

You can create a task using a specific wizard.

To launch the wizard:

1. Click the Tasks tab.
2. In left-hand pane, click New > Specific Tasks > Deploy Wizard. The wizard launches.

Deploying a Task

Select Item to Deploy Page

Select the name of a specific configuration from the list and enter a name for the task. If you do not assign a name, Wireless Manager appends TaskN to the end of the name of the selected configuration, where *N* is an incremental integer starting with 1.

Enter Task Name

In the Name field, enter a unique name for this task.

Select Targets and Deployment Time Page

1. In the Available Targets window, select the name of one or more Wireless Controllers, APs, AP groups, or AP Load Groups to apply the configuration. Deployment items to consider:

   - If you deploy a template to only one member of an availability pair, no synchronization will occur. If this is not what you intended, you must select both Wireless Controllers in the pair.

   - If a template is currently deployed to an availability pair and you only want to deploy to one of the Wireless Controllers in the pair, you must first undeploy on both.

- If an AP Group has no APs, or in the case of an AP Profile deployment it contains no APs of an appropriate hardware type, it is displayed as greyed out.

- Selecting any AP, AP Group, or AP Load Group automatically selects the parent Wireless Controller. This Wireless Controller cannot be deselected until all APs causing it to be selected have been deselected. When you try to deselect a Wireless Controller, if there are any targets making it a mandatory target, you will be informed of which ones they are, so that you can deselect them.

- Selecting an AP Group will result in all of its member APs and their Wireless Controllers being selected. If an AP is selected because an AP Group containing it is selected, it cannot be deselected until the AP Group is deselected.

2. To schedule the task deployment, select one of the following options:

   - Execute Immediately – Places the task in the queue to execute immediately, or as soon as possible if other tasks are already in the queue.

   - Do Not Execute – Stores the task for future execution.

   - Specify Time – Enables you to schedule task execution. You can select the date and time when you want the task to execute.

   - Enforce using Policy Manager – Enables you to enforce the template that references a PM-Policy or PM-CoS for the selected deployment targets.

3. Enter a Port or Mask for the Controller, if applicable. If the topology is part of a topology group, this displays all topologies in the group.

4. When deploying a template, if a suitable AP Group is not listed, click Add AP Group to create one.

   a. The Create New AP Group window displays

   b. In the Name field, enter the name of the new AP group.

   c. To include an AP into the named AP group, select an AP from the Available APs window and use the arrow key to move it into the APs in Group window. Use the Shift key to add multiple APs that are listed adjacent to each other; use the Ctrl key to add several APs that are not listed adjacent to each other. To remove an AP from the named AP group, select an AP in the APs in Group window and use the arrow key to move it into the Available APs window.

  d. Click **OK** to save the AP group or click **Cancel** to discard the AP group configuration.

Selecting Targets for VNS/WLAN Service Deployment

- The Change Radio Assignments check box only applies to APs, and AP Groups, and is only enabled when either of these is selected. As for radio assignments for AP Load Groups, these are specified as part of the AP Load Group definition.

- The Default WLAN Service Assignment check box is only enabled if 'Change Radio Assignments' is selected.

- An AP Load Group can only be selected as a valid target for deployment if it is synchronized. Moreover, you will not be allowed to re-deploy a template that was previously deployed to an AP Load Group and has become un-synchronized, until you first re-deploy the AP Load Group or delete it.

- Selecting an AP Group will result in all of its member APs and their Wireless Controllers being selected. Similarly, any radio assignments made to an AP Group will apply to all of its member APs. If you want to customize the radio assignments of any APs belonging to an AP Group that has radio assignments, you must first remove them from the AP Group.

- If the VNS/WLAN being deployed is a remotable VNS/WLAN then any Wireless Controllers implicitly represented by an AP, AP Group, or AP Load Group which are part of a Mobility Zone will be automatically selected.

For more information, see [About WLAN Service Templates](#) and [About Virtual Network Services (VNS) Templates](#).

Selecting Targets for Remotable VNS/WLAN Service Deployment

This page lists available target Wireless Controllers that can host the remotable WLAN in a Mobility Zone. Any stand-alone Wireless Controllers are listed for reference only and the selection is not editable. Select at least one Wireless Controller in each Mobility Zone where the template will be deployed as remotable.

Remotable WLAN templates are identified by selecting Remotable on the Advanced dialog within the WLAN Services Template page. For more information, see [Manually Creating a WLAN Service Template](#).

NOTE: When deploying a VNS, it is only deployed on those Wireless Controllers marked remotable. The remotable Wireless Controller also receives the remotable WLAN service for which the user may be prompted to specify per-Wireless Controller settings for Default Topology (see EWC Specific Topology Settings Page), RADIUS (see EWC Specific RADIUS Servers Settings Page) or captive portal (see EWC Specific Captive Portal Settings Page) during deployment. The other Wireless Controllers receive the remote WLAN service definition which does not include any per-controller Auth & Acct settings (see WLAN Service Template Configuration Page).

Remove a remotable template by clearing the target selection.

NOTE: Clearing the remotable Wireless Controller will not only remove the remotable Wireless Controller, but also remove all remote Wireless Controllers in the same Mobility Zone.

Verify Targets

This page provides a list of deployed targets (EWCs, APs, AP Groups, and AP Load Groups) for the selected template. Targets can be removed or additional targets can be added by clicking the Prev button and editing the selection as necessary.

Specifying EWC Specific Settings

EWC Specific Topology Settings Page

This page displays information about the target Wireless Controllers and enables you to customize their configurations. For more information, see Creating a Network Topology Configuration.

1. Select the name of the Wireless Controller that you want to customize.

2. Depending on the mode of the topology, the following per-controller settings can be configured:

- Bridged at EWC - port, interface IP, mask

    a. From the drop-down menu, select the physical multicast port to assign to the Wireless Controller.

    If the multicast port for a controller is changed, and the template is deployed successfully, the per-controller settings in all other templates referencing this property are updated accordingly.

- Routed - multicast, gateway, mask, DHCP

a. If available, click the Configure DHCP Settings button to configure DHCP. The DHCP Settings window displays.

b. Select from the following DHCP settings:

- None

- Use Relay

- Local Server

c. Click **Close** to close the DHCP Setting window.

EWC Specific RADIUS Servers Settings Page

This page displays information about the target RADIUS servers and enables you to customize their configurations.

1. Select the name of the Wireless Controller that you want to customize.

2. Under Controller, select a Wireless Controller priority.

3. From the drop-down menus, select the desired authentication and accounting configuration. For more information, see [Creating a RADIUS Server Definition](#).

EWC Specific Captive Portal Settings Page

This page displays information about Captive Portal servers and enables you to customize their configurations.

1. Select the name of the Wireless Controller that you want to customize.

2. Settings include:

    a) Firewall Friendly External: Redirection URL, FQDN for EWC IP, Default Redirection URL.

    b) Internal, Guest Portal, Guest Splash: Default Redirection URL, FQDN for Gateway IP.

    c) External: Redirection URL, IP Address, Port.

3. Click **Next**.

Controller Specific Radar Settings

This page displays information about Radar settings for both single controllers and availability pairs.

1. Under Single Controller, select whether or not to enable the Security Analysis Engine. For more information, see [About Radar](#).

2. Under Availability Pairs:

   - For controllers in availability running V9.15 or later software, select whether or not you wish to enable the Security Analysis Engine in each availability pair.

   - For controllers in availability running software prior to V9.15, only one controller should have the Security Analysis Engine enabled in each availability pair.

3. Click **Next**.

Verify AP Membership

This page displays APs that are members of a Guardian scan profile. When an AP is assigned to a Guardian scan profile it will stop providing forwarding services, or operating as a load group or site member. Any APs that show up in the "APs to be added" section of the "Verify AP Membership" dialog, once assigned to the guardian scan profile, will stop providing other services (WLAN Services, Load Groups, and Sites). Any APs that show up in the "APs to be removed" section of this dialog, upon deployment will have their corresponding services re-instated.

1. Click the Tasks tab.

2. In left-hand pane, click New > Radar Tasks > Deploy Guardian Scan Profile. The wizard launches.

3. On the Verify AP Membership dialog, expand the tree for the desired controller.

4. Click **Next**.

Execute Task Page

A message displays stating whether the task was successfully deployed. Click close to close the window or click View Log to view detailed log information about the task.

Deploying Point of Presence in Extreme Management Center (Legacy)

The Point of Presence wizard provides the ability to change the point of presence of a Policy Manager enforced role on a controller. When a new PM role is enforced on a controller, AP Filtering is enabled by default.

Using this wizard you can change this setting subject to the following restrictions.

- If a role references a B@AP topology (in policy rules, default access control, or egress VLANs) the controller automatically enables AP Filtering.
- If a role's option "Allow action in policy rules, contains to the VLAN assigned by the role." is selected then WM will allow the user to configure "Custom AP Filtering".

Deploying WLAN Service Assignments in Bulk in Extreme Management Center (Legacy)

The bulk WLAN service assignment wizard allows you to assign one or more (already deployed) WLAN Service templates to the radios of APs, AP Groups, or AP Load Groups.

1. **Enter Task Name.** In the Name field, enter a unique name for this task.

2. **Select WLAN Services.** Select the WLAN service templates on which to modify radio assignments. You must select at least one WLAN service template. For more information, see [Creating a WLAN Service Template](#).

3. **Select Targets.** Select one or more Wireless Controllers, APs, AP groups, or AP Load Groups to apply the configuration.

4. **Modify Radio Assignments.** This page shows the current WLAN-Radio assignments for each AP, AP Group, and AP Load Group.

   - For AP Load Groups, click the desired square to change the assignment of the WLAN on the AP Load Group.

   - For APs and AP Groups, you can modify the assignments by selecting the radios and then clicking the desired WLAN-AP intersections in the table.

5. **Execute Task.** A message displays stating whether the task was successfully deployed. Click **Close** to close the window or click **View Log** to view detailed log information about the task.

Monitoring Tasks in Extreme Management Center (Legacy)

After you create tasks, Wireless Manager stores task definitions for historical purposes and so that you can view the list of tasks and their current status, copy, or edit the tasks.

Because tasks are associated with a large volume of data, only a limited number of them can be retained. You can configure the number of executed tasks to be retained for historical purposes in Wireless Manager's options. Wireless Manager enforces this restriction by a nightly cleanup process.

You can view detailed historical information about all tasks created, including the actual CLI scripts executed by the task and the data actually deployed by the task as part of the task definition.

For general information about tasks, go to Managing Tasks.

This Help topic includes the following information:

- Viewing Task Status and Historical Summary Information
- Viewing Task Details
- Editing a Task
- Deleting a Task
- Rescheduling a Task

Viewing Task Status and Historical Summary Information

You can view status and historical summary information about all tasks created from the Task Summary page.

To view the Task Summary page:

1. Click the Tasks tab.
2. In left-hand pane, click Task management > Task History. The Task Summary page displays.

The following list describes the information available on the Task Summary page.

Status

- Status of the task. Options include:

- Not scheduled — Task is created but has not yet executed or been scheduled to execute.

- Pending — The task is scheduled but has not yet executed.

- Pending Failure – The task is scheduled but has not yet executed, however due to incompatible targets it is expected to fail.

- Partial success — The task finished executing but did not completely succeed. It may not have been deployed to one of the targets or only partially deployed on a target.

- Running — Task is currently executing.

- Success — The task finished executing successfully on all targets.

- Failed — Task execution failed completely.

- Deleting — Task is currently being deleted.

ID

A numeric string that identifies the order in which the task was created. For example, ID 1 identifies this as the first task created. ID 10 identifies it as the tenth task created.

Name

Name associated with the task. When a task is created, you can assign a name to the task or Wireless Manager will assign a name for you by appending TaskN to the name of the object the task will deploy.

Task Type

The type of task. Options are Policy, VNS, AP Profile, WLAN service, WLAN assignment, RADIUS, Topology, Rate Profile, Classes of Service, and Load Group.

Created

Date the task was created.

Scheduled

Identifies:

- whether the task has already executed

- whether the task is scheduled to execute

- the time and date of task that is scheduled to execute.

Creator

Name of the user who created the task.

Toolbar Buttons

For a description of common toolbar buttons see <u>Context-Sensitive Toolbar</u>.

Viewing Task Details

You can view detailed information about a specific task from the Task Details page for that task.

To view the Task Details page:

1. Click the Tasks tab.

2. In left-hand pane, click Task management > Task Details. The Task Details page displays.

3. In the left-hand pane, click on a Task Name from the list. The Task Details page for that task displays.
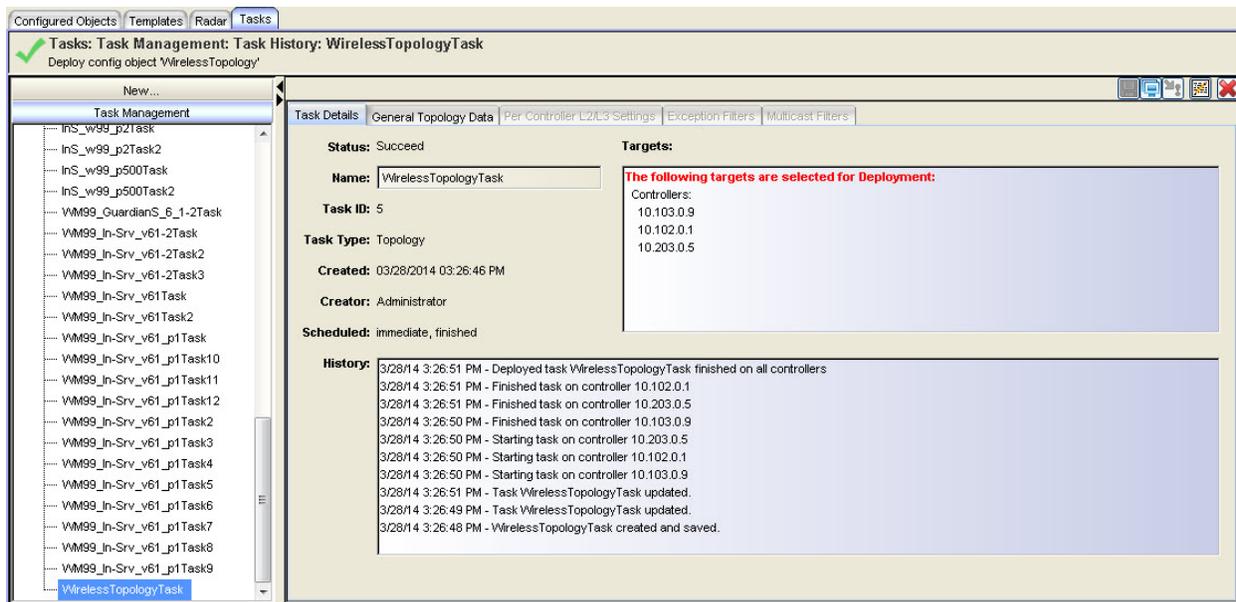
The following list describes the information available on the Task Details page.

Task Details Tab

Status

Status of the task. Options include:

- Not scheduled — Task is created but has not yet executed or been scheduled to execute.

- Pending — The task is scheduled but has not yet executed.

- Pending Failure – The task is scheduled but has not yet executed, however due to incompatible targets it is expected to fail.

- Partial success — The task finished executing but did not completely succeed. It may not have been deployed to one of the targets or only partially deployed on a target.

- Running — Task is currently executing.

- Success — The task finished executing successfully on all targets.

- Failed — Task execution failed completely.

- Deleting — Task is currently being deleted.

Name

Name associated with the task. When a task is created, you can assign a name to the task or Wireless Manager will assign a name for you by appending TaskN to the name of the object the task will deploy.

Task ID

A numeric string that identifies the order in which the task was created. For example, ID 1 identifies this as the first task created. ID 10 identifies it as the tenth task created.

Task Type

The type of task. Options are Policy, VNS, AP Profile, WLAN service, WLAN assignment, RADIUS, Topology, Rate Profile, Classes of Service, and Load Group.

Created

Date the task was created.

Creator

Name of the user who created the task.

Scheduled

Identifies:

- whether the task has already executed.
- whether the task is scheduled to execute.
- the time and date of task that is scheduled to execute.

History

The history lists significant events in the life of the task, including:

- When it was created.
- When it was changed.
- When it was deployed.

Targets

Wireless Controllers, APs, AP Groups, or AP Load Groups to which the template will be applied.

Toolbar Buttons

For a description of common toolbar buttons see <u>Context-Sensitive Toolbar</u>.

Editing a Task

You can edit a task to change the configurable information. This information differs depending on the template type or configured object type.

To edit a task:

1. Click the Tasks tab.

2. Select a task and either click the edit icon at the top of the page or right-click on the task name and select Edit from the drop-down menu. The Task Details page displays.

3. Configure individual settings as needed. The Task Details Page - Fields and Buttons table describes the information available on the Task Details page.

4. Click **Save**.

Deleting a Task

You can delete a task as long as it is not currently executing.

To delete a task:

1. Click the Tasks tab.

2. Select a task and either click the delete icon at the top of the page or right-click on the task name and select Delete from the drop-down menu. A confirmation dialog box displays.

3. Click **Yes** to delete the task. The Task Details page displays with the updated information.

Rescheduling a Task

You can reschedule a task as long as it has not already executed.

To reschedule a task:

1. Click the Tasks tab.

2. Select a task on the Task Summary page and either click the reschedule icon at the top of the page or right-click on the task name and select Reschedule from the drop-down menu. The Reschedule Task wizard launches.

Reschedule Tasks Wizard

Select the New Deployment Time Page

1. In the Select new Deployment Time window, select a time for task deployment. Options include:

- Execute Immediately – Places the task in the queue to execute immediately, or as soon as possible if other tasks are already in queue.

- Specify Time – Enables you to schedule task execution. You can select the date and time when you want the task to execute.

2. Click **Next**.

Execute Task Page

A message displays stating whether the task was successfully deployed.

Click **Close** to close the window or click **View Log** to view detailed log information about the task.