
# Access Point

*WiNG 7.1.0 System Reference Guide*

9036127-00

Published March 2019

## Legal Notice

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

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

## Trademarks

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

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

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

# Table of Contents

# Preface

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

## Text Conventions

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

**Table 1: Notice Icons**

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

**Table 2: Text Conventions**

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

## Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by ExtremeXOS software, which are the following:

- ExtremeSwitching® switches
- Summit® switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the ExtremeXOS command documentation (see the Extreme Documentation page at www.extremenetworks.com/documentation/). In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines sections.

## Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

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

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

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

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

## Getting Help

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

| | |
|---|---|
| Extreme Portal | Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications. |
| The Hub | A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC. |
| Call GTAC | For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact |

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

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)

- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

### Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).
3 Select the products for which you would like to receive notifications.

**Note**
You can modify your product selections or unsubscribe at any time.

4 Click **Submit**.

## Documentation and Training

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

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

### Training

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

# 1 About this Guide

**Heterogeneous AP Management**
**Notational Conventions**

This manual describes how to use the *Graphical User Interface* (GUI) to configure settings required to deploy Extreme Networks access points within a WiNG 7.1.0 (hereafter referred to as WiNG 7.1) managed network.

The WiNG 7.1 software, at launch, supports the following access points and service platforms:

- Access Points — AP505i, AP510i
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

The AP505i and AP510i model access points are new *access points* (APs) introduced in the WiNG 7.1 release.

- AP505i - This is a next generation, enterprise-class 802.11ax access point. The “i” in AP505i indicates that it comes with internal antennas. The AP505i can be used in stadiums, public venues such as hospitals and hotels, retail industry, and educational institutions. The 802.11ax technology supports more users and *internet of things* (IoT) devices.
- AP510i - This is a next generation, enterprise-class 802.11ax access point. The “i” in AP510i indicates that it comes with internal antennas. The AP features a dual-band radio, a band locked radio, and comes with eight (8) WiFi internal antennas and one *Bluetooth Low Energy* (BLE) antenna.

Note
Both AP505i and AP505i require a minimum base firmware of WiNG 7.1 and can adopt to a WiNG 7.1 enabled Controller and Virtual Controller, or ExtremeCloud Appliance.

## Heterogeneous AP Management

This section describes the WiNG 5.9.X access points capability of being deployed as *virtual controllers* (VCs). It also provides an overview of heterogeneous adoption.

The family of supported access points enable high performance with secure and resilient wireless voice and data services to remote locations with the scalability required to meet the needs of large distributed enterprises.

The AP7522, AP7532, AP7562, AP7632, AP7662, AP8543 and AP8533 model access points can now use WiNG software as its on-board operating system. The unique software enables the access point to function as a Standalone “thick” access point, or a virtual controller AP capable of adopting and managing up to 64 other access points.

The AP7502, AP7602, AP7612, AP7622 and AP8163 model access points can now use WiNG software as its on-board operating system. The unique software enables the access point to function as a Standalone “thick” access point, or a virtual controller AP capable of adopting and managing up to 24 access points.

The WiNG heterogeneous AP management feature enables access points to adopt and manage different types of AP model when functioning as a virtual controller.

Note
A higher family AP can manage a lower family AP whereas, a lower family AP cannot manage a higher family AP.

The following hierarchy is supported:

- AP8432/AP8533 can manage AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8432 and AP8533.
- AP7662/AP7632 can manage AP7662, AP7632, AP7622, AP7612, and AP7602.

The following hierarchy is not supported:

- AP7522/AP7532/AP7562 support for AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662.
- AP7632/AP7622 support for AP7522, AP7532, AP7562.

Note
AP6522 and AP6562 are not currently equipped to adopt to managing up to 64 access points of the same model. Only access points on WAVE-1 and WAVE-2 platforms can adopt and manage 64 APs.

When deploying an access point as a pure virtual controller AP, with no RFS Series controllers available anywhere on the network, the access point itself is a controller supporting other access points of the same model. The virtual controller AP can:

- Provide firmware upgrades for connected access point.
- Aggregate statistics for the group of access points the virtual controller is managing.
- Be the single point of configuration for that deployment location.

The recommended way to administer a network populated by numerous access points is to configure them directly from the virtual controller AP. If a single access point configuration requires an update from the virtual controller AP's assigned profile configuration, the administrator should apply a device override to change just that access point's configuration. For more information on applying an override to an access point's virtual controller AP assigned configuration and profile, see Device Profile Overrides on page 322 .

The WiNG architecture is a solution designed for 802.11n and 802.11ac networking. It leverages the best aspects of independent and dependent architectures to create a smart network that meets the connectivity, quality and security needs of each user and their applications, based on the availability of network resources including wired networks. By distributing intelligence and control amongst access points, a WiNG network can route directly via the best path, as determined by factors including the user, location, the application and available wireless and wired resources. WiNG extends the differentiation offered to the next level, by making available services and security at every point in the network. managed traffic flow is optimized to prevent wired congestion and wireless congestion. Traffic flows

dynamically, based on user and application, and finds alternate routes to work around network choke points.

Note

The WiNG 7.1 AP505 and AP510 model access points can be deployed as virtual controllers. However, heterogeneous adoption is not supported. An AP505 can only adopt another AP505. And an AP510 can only adopt another AP510 model access point.

## Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents
- Bullets (•) indicate:
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
  - action items
- Sequential lists (those describing step-by-step procedures) appear as numbered lists

# 2 Introduction

**WiNG 7.1.0 Operating System Overview**

This chapter provides a general overview of the WiNG 7.1 operating system.

## WiNG 7.1.0 Operating System Overview

The WiNG 7.1 operating system is a solution designed for 802.11n, 802.11ac and 802.11ax networking. It is a convergence of the legacy ExtremeWireless™ WiNG (5.9.X) and ExtremeWireless™ (10.X) wireless operating systems. It offers a high-level of flexibility and scalability covering both campus and distributed modes of deployment.

WiNG 7.1 brings together the following key benefits of both deployment topologies under one fold:

- ExtremeWireless - The ExtremeWireless software provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11 standard. The system is intended for enterprise networks operating on multiple floors in more than one building, and is ideal for public environments, such as airports and convention centers that require multiple access points. It is an ideal solution for high-density, campus and stadium deployments. It is well suited to meet the needs of enterprises in the education, healthcare, sports and entertainment verticals. The ExtremeWireless OS key strengths are:
  - Extensive Policy Framework
  - Contextual Device and Application Control
  - Application Visibility & Control with Analytics
  - BYOD - Single SSID with Programmable Data Path
  - Voice & Video Optimized with Seamless Roaming
- ExtremeWireless WiNG - The WiNG architecture is a solution designed for 802.11n and 802.11ac networking. It is designed for standalone or distributed hierarchical networks. The ExtremeWireless WiNG software distributes intelligence right to the network edge, empowering every controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time. It is highly scalable and well suited to meet the needs of large, geographically distributed enterprises. It is an ideal wireless networking solution for the retail, manufacturing, transportation & logistics, and hospitality verticals. The ExtremeWireless OS key strengths are:
  - Simple Guest Access with Analytics
  - Contextual Application Control
  - Advanced Diagnostics and Remote Troubleshooting
  - Intrusion, Compliance and WiFi Forensics
  - Scale-out 1000s of APs with Rapid Rollout
  - Self-tuning RF (Smart-RF)
  - Distributed Service Intelligence

Going forward, this unified, common, wireless, infrastructure WiNG 7.1 OS will power both ExtremeWireless and ExtremeWireless WiNG product families. At launch, the following platforms will be supported:

- Access Points - AP510i, AP505i
- Service Platform - NX5500, NX7500, NX9500, NX9600, and VX9000

## Interoperability with WiNG 5.9.X

Interoperability with access points running the WiNG 5.9.X OS is another salient feature of the WiNG 7.1 OS. As part of this inter-interoperability, WiNG 7.1 wireless controllers and service platforms are capable of deploying and managing the following WiNG 5.9.X APs:

- Access Points - AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP763, AP7662, AP8163, AP8543, AP8533

## Dual Mode Capability

The WiNG 7.1 AP505 and AP510 model access points have the capability of operating in the following two modes: **`Distributed`** and **`Centralized`**. For a newly-manufactured, out-of-the-box AP505 and AP510 model access point the mode of operation is not specified.

Note
For more information, see Dual Mode Capability.

## AP510i Specifications

The enterprise class 802.11ax AP501i access point has the following features:

- Radios: 2 radios; 1 IoT radio (2.4 GHz).
- Console Port: RJ45.
- Two Ethernet Ports:
  - GE1 - 10/100/1000/2500/5000 Mbps auto-negotiation Ethernet port, RJ45, with *Power over Ethernet* PoE In
  - GE2 - 10/100/1000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
- LEDs: 6 – All LEDs will be on during reset
- One Reset button
- Power: PoE 802.3af; 12VDC external power in connector.
- Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

Note
For more information, please refer to the AP510i installation guide, available at https://extremenetworks.com/documentation.

## AP505i Specifications

The enterprise class 802.11ax AP505i access point has the following features:

- Radios: 2 radios (one band locked at 2.4 GHz and the other band at 5 GHz); 1 IoT radio (2.4 GHz)
- Console port: RJ45
- Two Ethernet ports:
  - GE1 - 10/100/1000/2500 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
  - GE2 - 10/100/1000 Mbps auto-negotiation Ethernet port, RJ45, with NO PoE
- LEDs: 6 LEDs; all LEDs will be on during reset
- One reset button
- Power: PoE 802.3af; 12VDC external power in connector
- Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

Note
For more information, please refer to the AP505i installation guide, available at https://extremenetworks.com/documentation.

## About the WiNG Software

Extreme Networks' WiNG operating system is the next generation in the evolution of WLAN architectures. This OS is designed to scale efficiently from the smallest networks to large, geographically dispersed deployments. The co-operative, distributed control plane innovation in the WiNG architecture offers a *software-defined networking* (SDN)-ready operating system that can distribute controller functionality to every access point in your network. Now, every access point is network aware, providing the intelligence required to truly unleash optimal performance, all wireless LAN infrastructure can work together to ensure every transmission is routed through the most efficient path, every time.

The WiNG OS brings you the resiliency of a standalone access point network without the vulnerability of a centralized controller, with advancements that take performance, reliability, security, scalability and manageability to a new level. The result? Maximum network uptime and security with minimal management. And true seamless and dependable mobility for your users.

WiNG OS advances the following technology:

Comprehensive Wi-Fi support - WiNG supports all Wi-Fi protocols, including 802.11a/b/g/n/ac/ax, allowing you to create a cost-effective migration plan based on the needs of your business.

Extraordinary scalability - With WiNG, you can build any size network, from a small WLAN network in a single location to a large multi-site network that reaches all around the globe.

Extraordinary flexibility - No matter what type of infrastructure you deploy, WiNG OS delivers intelligence to all: standalone independent access points or adaptive access points that can be adopted by a controller but can switch to independent mode; virtual controllers; physical controllers in branch offices, the NOC *(network operating center)* or the cloud.

Distributed intelligence - WiNG distributes intelligence right to the network edge, empowering every controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time.

Extraordinary network flexibility and site survivability - WiNG provides the best of both worlds: true hierarchical management that delivers a new level of management simplicity and resiliency by enabling controllers to adopt and manage other controllers and access points, while allowing adopted infrastructure to also stand on its own.

Gap-free security - When it comes to security, there can be no compromises. WiNG's comprehensive security capabilities keep your network and your data safe, ensuring compliance with PCI, HIPAA and other government and industry security regulations.

Connectivity for large indoor and outdoor spaces - In addition to enabling a robust indoor WLAN, our patented MeshConnex™ technology enables the extension of Wi-Fi networks to the largest of outdoor spaces from an expansive outdoor campus environment to an entire city.

Powerful centralized management - With WiNG you get complete control over every aspect of your WLAN. This single powerful windowpane enables zero touch infrastructure deployment, rich analytics that can help you recognize and correct brewing issues before they impact service quality and user connectivity, along with centralized and remote troubleshooting and issue resolution of the entire network.

Application visibility and control -

With WiNG you get visibility & control over layer-7 applications with an embedded *Deep Packet Inspection* DPI engine that inspects every flow of every user at the access point. The embedded DPI engine in the WiNG OS is capable of detecting and identifying thousands of applications real time. You can configure your access points to report this real-time, network statistics to the Extreme NSight. Network administrators can get in-depth insight into every dimension of the network including layer-7 application visibility, client devices, device & OS types and users. Administrators can discern, at a glance, the top applications by usage or by count at every level of the network from site level to access points and clients. In addition to detection, firewall and QoS policies can leverage the application context to enforce policies.

### *Distributed Intelligence*

WiNG OS enables all WLAN infrastructure with the intelligence required to work together to determine the most efficient path for every transmission. The need to route all traffic through a controller is eliminated, along with the resulting congestion and latency, resulting in higher throughput and superior network performance. Since all features are available at the access layer, they remain available even when the controller is offline, for example, due to a WAN outage, ensuring site survivability and extraordinary network resilience. In addition, you get unprecedented scalability, large networks can support as many as 10,000 nodes without impacting throughput or manageability, providing unprecedented scalability.

### *High Availability Networks*

The WiNG OS enables the creation of highly reliable networks, with several levels of redundancy and failover mechanisms to ensure continuous network service in case of outages. APs in remote sites coordinate with each other to provide optimized routing and self-healing, delivering a superior quality of experience for business critical applications. Even when WiNG site survivable APs lose communication with the controller, they continue to function, able to bridge traffic while still enforcing QoS and security policies, including stateful inspection of Layer2 (locally bridged) or Layer 3 traffic.

*Gap-free Security*

When it comes to wireless security, one size does not fit all. A variety of solutions are required to meet the varying needs and demands of different types of organizations. Regardless of the size of your WLAN or your security requirements, our tiered approach to security allows you to deploy the features you need to achieve the right level of security for your networks and your data. And where a hub-and-spoke architecture can't stop threats until they reach the controller inside your network, WiNG OS distributes security features to every access point, including those at the very edge of your network, creating an around-the-clock constant network perimeter guard that prevents threats from entering your network for unprecedented gap free security.

*Outdoor Wireless and Mesh Networking*

When you need to extend your wireless LAN to outdoor spaces, our patented MeshConnex technology combines with comprehensive mesh networking features to enable you to create secure, high performance, flexible and scalable mesh networks. With our mesh technology, you can cover virtually any area without installing cabling, enabling the creation of cost-effective outdoor wireless networks that provide coverage to enterprise workers in vast campus-style environments as well as public safety personnel in patrol cars.

*Network Services, Routing and Switches*

The WiNG OS integrates network services like built-in DHCP server, AAA server and routing protocols like policy based routing and OSPF, Layer 2 protocols like MSTP and Link Aggregation. Integration of services and routing/ switching protocols eliminates the need for additional servers or other networking gear in small offices thereby reducing *Total Cost of Ownership* (TOC). In large networks, where such services are deployed on a dedicated server/ router at the NOC, this provides a backup solution for remote sites when the WAN link to the NOC is temporarily lost. Integrating also provides the added benefit of coordination across these services on failover from primary to standby, assisting a more meaningful behavior, rather than when each fails over independently of the other for the same root cause.

*Management, Deployment and Troubleshooting*

The WiNG OS is a comprehensive, end-to-end management system that covers deployment through day-to-day management. You get true zero-touch deployment for access points located anywhere in the world, the simplicity of a single window into the entire network, plus the ability to remotely troubleshoot and resolve issues. And since our management technology is manufacturer-agnostic, you can manage your Extreme Networks WLAN infrastructure as well as any legacy equipment from other manufacturers, allowing you to take advantage of our advanced WLAN infrastructure without requiring a costly rip and replace of your existing WLAN.

# 3 Web UI Features

**Accessing the Web UI**
**Glossary of Icons Used**

The access point's on board user interface contains a set of features specifically designed to enable either Virtual Controller AP, Standalone AP or Adopt to Controller functionality. In Virtual Controller AP mode, an access point can adopt and manage other access points. With the introduction of Heterogeneous AP management, access points are able to adapt and manage different types of AP model when functioning as a virtual controller. In Standalone mode, an access point functions as an autonomous, non adopted, access point servicing wireless clients. If adopted to controller, an access point is reliant on its connected controller for its configuration and management.

For information on how to access and use the Web UI, see:


- Accessing the Web UI on page 17.
- Glossary of Icons Used on page 19.


## Accessing the Web UI

Access points, controllers and service platforms use a GUI that can be accessed using any supported Web browser on a client connected to the subnet the Web UI is configured on.

### Browser and System Requirements

To access the GUI, a browser supporting Flash Player 11 is recommended. The system accessing the GUI should have a minimum of 1 GB of RAM for the UI to display and function properly, with the exception of NX service platforms, which require 4 GB of RAM. The Web UI is based on Flex, and does not use Java as the underlying UI framework. A resolution of 1280 x 1024 pixels for the GUI is recommended.

The following browsers are required to access the WiNG Web UI:

- Firefox 3.5 or higher
- Internet Explorer 7 or higher
- Google Chrome 2.0 or higher
- Safari 3 and higher
- Opera 9.5 and higher

Note
Throughout the Web UI, leading and trailing spaces are not allowed in any text fields. In addition, the "?" character is also not supported in text fields.

## Connecting to Web UI

Follow the steps below to connect to an *access point's* (AP's) Web UI for the first time:

1 Connect one end of an Ethernet cable to the AP's LAN port and connect the other end to a computer with a working Web browser.

2 Set the computer to use an IP address between 192.168.0.10 and 192.168.0.250 on the connected port. Set a subnet/network mask of 255.255.255.0.

The AP's IP address is optimally provided using DHCP. A zero config IP address can also be derived if DHCP resources are unavailable. Using zero config, the last two octets in the IP address are the decimal equivalent of the last two bytes in the access point's hard-coded MAC address.

Deriving the AP's IP address using its MAC address.

If the AP's hard-coded MAC address is 00:C0:23:00:F0:0A, follow the steps below to derive the AP's Zero-config IP address:

a On your computer, open the Windows calculator. To access the calculator, click **Start → All Programs → Accessories → Calculator**. This path may vary depending on the version of Windows running on your computer.

b With the Calculator displayed, select **View → Scientific** or **View → Programmer** depending on the version of Windows running on your computer.

c Select the **Hex** radio button.

d Enter the penultimate octet of the AP's MAC address. In this example, the AP's MAC address is: *00:C0:23:00:F0:0A*. Enter `F0`.

e Select the **Dec** radio button. The calculator converts F0 into 240.

f Repeat this process for the last octet in the AP's MAC address. Enter `A`, and select **Dec**. The calculator converts A into 10.

The AP's zero-config IP address is: 169.254.240.10

3 Once obtained, point the Web browser to the access point's IP address. The following login screen displays:

The Web UI login dialog displays:

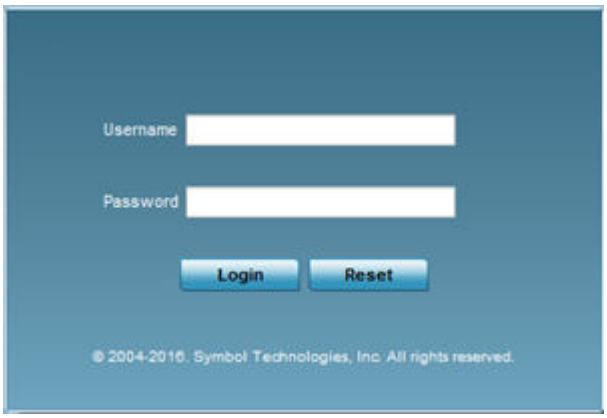



**Figure 1: Web UI Login Screen**

4 Enter the default username `admin` in the Username field.

5 Enter the default password `admin123` in the **Password** field.

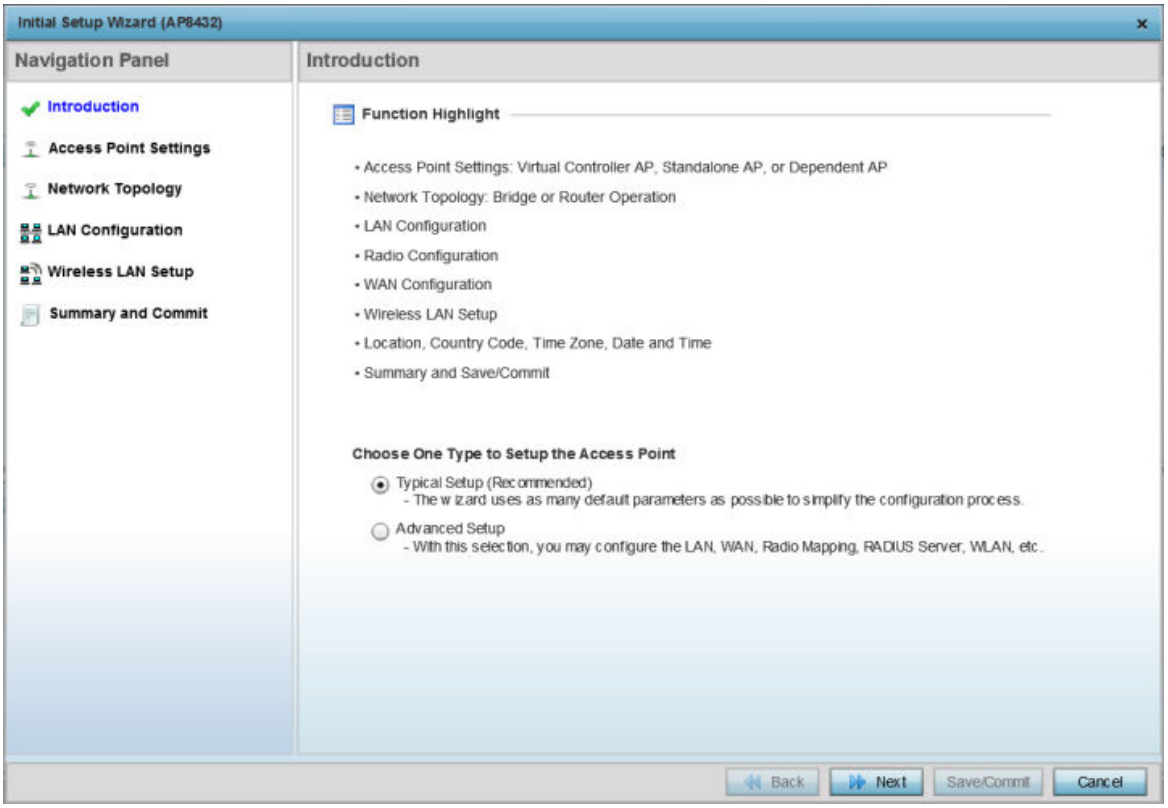
When logging in for the first time, you will be prompted to change the password to enhance device security. Set the new password and use it for subsequent logins.

6 Click the **Login** button to load the device's (access point, wireless controller or service platform) management interface.

If you are powering-up the AP for the first time, the AP's management UI opens, and the **Initial Setup Wizard** dialog pops up. Use this wizard to configure the basic settings required to get the AP up and running. For more information on using the Initial Setup Wizard, see Using the Initial Setup Wizard on page 25.

The AP's Initial Setup Wizard:

**Figure 2: The Initial Setup Wizard**




## Glossary of Icons Used

The UI uses a number of icons used to interact with the system, gather information, and obtain status for the entities managed by the system. This chapter is a compendium of the icons used. This chapter is organized as follows:

- Global Icons
- Dialog Box Icons
- Table Icons
- Status Icons
- Configurable Objects

- Configuration Objects
- Configuration Operation Icons
- Access Type Icons
- Administrative Role Icons
- Device Icons

## Global Icons

This section lists global icons available throughout the interface.

| | |
|---|---|
|  | *Logout* – Select this icon to log out of the system. This icon is always available and is located at the top right corner of the UI. |
|  | *Add* – Select this icon to add a row in a table. When selected, a new row is created in the table or a dialog box displays where you can enter values for a particular list. |
|  | *Delete* – Select this icon to remove a row from a table. When selected, the selected row is deleted. |
|  | *More Information* – Select this icon to display a pop up with supplementary information that may be available for an item. |
|  | *Trash* – Select this icon to remove a row from a table. When selected, the row is immediately deleted. |
|  | *Create new policy* – Select this icon to create a new policy. Policies define different configuration parameters that can be applied to individual device configurations, profiles and RF Domains. |
|  | *Edit policy* – Select this icon to edit an existing configuration item or policy. To edit a policy, select a policy and this icon. |

## Dialog Box Icons

These icons indicate the current state of various controls in a dialog. These icons enables you to gather the status of all the controls in a dialog. The absence of any of these icons next to a control indicates the value in that control has not been modified from its last saved configuration.

| | |
|---|---|
|  | *Entry Updated* – Indicates a value has been modified from its last saved configuration. |
|  | *Entry Update* – States that an override has been applied to a device profile configuration. |
|  | *Mandatory Field* – Indicates this control value is a mandatory configuration item. You are not allowed to proceed further without providing all mandatory values in this dialog. |
|  | *Error in Entry* – Indicates there is an error in a supplied value. A small red popup provides a likely cause of the error. |

## Table Icons

The following two override icons are status indicators for transactions:

| | |
|---|---|
|  | *Table Row Overridden* – Indicates a change (profile configuration override) has been made to a table row and the change will not be implemented until saved. This icon represents a change from this device's profile assigned configuration. |
|  | *Table Row Added* – Indicates a new row has been added to a table and the change is not implemented until saved. This icon represents a change from this device's profile assigned configuration. |

## Status Icons

These icons indicate device status, operations, or any other action that requires a status returned to the user.

| | |
|---|---|
|  | *Fatal Error* – States there is an error causing a managed device to stop functioning. |
|  | *Error* – Indicates an error exits requiring intervention. An action has failed, but the error is not system wide. |
|  | *Warning* – States a particular action has completed, but errors were detected that did not prevent the process from completing. Intervention might still be required to resolve subsequent warnings. |
|  | *Success* – Indicates everything is well within the network or a process has completed successfully without error. |
|  | *Information* – This icon always precedes information displayed to the user. This may either be a message displaying progress for a particular process, or just be a message from the system. |

## Configurable Object Icons

These icons represent configurable items within the UI.

| | |
|---|---|
|  | *Device Configuration* – Represents a configuration file supporting a device category (access point, wireless controller etc.). |
|  | *Auto Provisioning Policy* – Represents a provisioning policy. Provisioning policies are a set of configuration parameters that define how access points and wireless clients are adopted and their management configuration supplied. |
|  | *Critical Resource Policy* – States a critical resource policy has been applied. Critical resources are resources whose availability is essential to the network. If any of these resources is unavailable, an administrator is notified. |
|  | *Wireless LANs* – States an action impacting a managed WLAN has occurred. |
|  | *WLAN QoS Policy* – States a *quality of service policy* (QoS) configuration has been impacted. |
|  | *Radio QoS Policy* – Indicates a radio's QoS configuration has been impacted. |
|  | *AAA Policy* – Indicates an *Authentication, Authorization and Accounting* (AAA) policy has been impacted. AAA policies define RADIUS authentication and accounting parameters. |
|  | *Association ACL* – Indicates an *Access Control List* (ACL) configuration has been impacted. An ACL is a set of configuration parameters either allowing or denying access to network resources. |

| | |
|---|---|
|  | *Smart RF Policy* – States a Smart RF policy has been impacted. Smart RF enables neighboring access point radios to take over for an access point radio if it becomes unavailable. This is accomplished by increasing the power of radios on nearby access points to compensate for the coverage hole created by the non-functioning access point. |
|  | *Profile* – States a device profile configuration has been impacted. A profile is a collection of configuration parameters used to configure a device or a feature. |
|  | *Bridging Policy* – Indicates a bridging policy configuration has been impacted. A bridging policy defines which VLANs are bridged, and how local VLANs are bridged between the wired and wireless sides of the network. |
|  | *RF Domain* – States an RF Domain configuration has been impacted. |
|  | *Firewall Policy* – Indicates a firewall policy has been impacted. Firewalls provide a barrier that prevents unauthorized access to resources while allowing authorized access to external and internal resources. |
|  | *IP Firewall Rules* – Indicates an IP firewall rule has been applied. An IP based firewall rule implements restrictions based on the IP address in a received packet. |
|  | *MAC Firewall Rules* – States a MAC based firewall rule has been applied. A MAC based firewall rule implements network allowance restrictions based on the MAC address in a received data packet. |
|  | *Wireless Client Role* – Indicates a wireless client role has been applied to a managed client. The role could be either sensor or client. |
|  | *WIPS Policy* – States the conditions of a WIPS policy have been invoked. WIPS prevents unauthorized access to the network by checking for (and removing) rogue access points and wireless clients. |
|  | *Device Categorization* – Indicates a device categorization policy has been applied. This is used by the intrusion prevention system to categorize access points or wireless clients as either sanctioned or unsanctioned devices. This enables devices to bypass the intrusion prevention system. |
|  | *Captive Portals* – States a captive portal is being applied. Captive portal is used to provide temporary controller, service platform or access point access to requesting wireless clients. |
|  | *DNS Whitelist* – A DNS whitelist is used in conjunction with captive portal to provide access to requesting wireless clients. |
|  | *DHCP Server Policy* – Indicates a DHCP server policy is being applied. DHCP provides IP addresses to wireless clients. A DHCP server policy configures how DHCP provides IP addresses. |
|  | *RADIUS Group* – Indicates the configuration of RADIUS group has been defined and applied. A RADIUS group is a collection of RADIUS users with the same set of permissions. |
|  | *RADIUS User Pools* – States a RADIUS user pool has been applied. RADIUS user pools are a set of IP addresses that can be assigned to an authenticated RADIUS user. |
|  | *RADIUS Server Policy* – Indicates a RADIUS server policy has been applied. A RADIUS server policy is a set of configuration attributes used when a RADIUS server is configured for AAA. |
|  | *Management Policy* – Indicates a management policy has been applied. Management policies configure access control, authentication, traps and administrator permissions. |
|  | *BGP – Border Gateway Protocol* (BGP) is an inter-ISP routing protocol which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. |

## Configuration Object Icons

These configuration icons are used to define the following:

| | |
|---|---|
|  | *Configuration* – Indicates an item capable of being configured by an interface. |
|  | *View Events / Event History* – Defines a list of events. Click this icon to view events or view the event history. |
|  | *Core Snapshots* – Indicates a core snapshot has been generated. A core snapshot is a file that records status events when a process fails on a wireless controller or access point. |
|  | *Panic Snapshots* – Indicates a panic snapshot has been generated. A panic snapshot is a file that records status when a wireless controller or access point fails without recovery. |
|  | *UI Debugging* – Select this icon/link to view current NETCONF messages. |
|  | *View UI Logs* – Select this icon/link to view the different logs generated by the UI, FLEX and the error logs. |

## Configuration Operation Icons

The following operations icons are used to define configuration operations:

| | |
|---|---|
|  | *Revert* – When selected, any unsaved changes are reverted to their last saved configuration settings. |
|  | *Commit* – When selected, all changes made to the configuration are written to the system. Once committed, changes cannot be reverted. |
|  | *Commit and Save* – When selected, changes are saved to the configuration. |

## Access Type Icons

The following icons display a user access type:

| | |
|---|---|
|  | *Web UI* – Defines a Web UI access permission. A user with this permission is permitted to access an associated device's Web UI. |
|  | *Telnet* – Defines a TELNET access permission. A user with this permission is permitted to access an associated device using TELNET. |
|  | *SSH* – Indicates a SSH access permission. A user with this permission is permitted to access an associated device using SSH. |
|  | *Console* – Indicates a console access permission. A user with this permission is permitted to access an associated device using the device's serial console. |

## Administrative Role Icons

The following icons identify the different administrative roles allowed on the system:

| | |
|---|---|
|  | *Superuser* – Indicates superuser privileges. A superuser has complete access to all configuration aspects of the connected device. |
|  | *System* – States system user privileges. A system user is allowed to configure general settings, such as boot parameters, licenses, auto install, image upgrades etc. |

| | |
|---|---|
|  | *Network* – Indicates network user privileges. A network user is allowed to configure wired and wireless parameters, such as IP configuration, VLANs, L2/L3 security, WLANs and radios. |
|  | *Security* – Indicates security user privileges. A security level user is allowed to configure all security related parameters. |
|  | *Monitor* – Defines a monitor role. This role provides no configuration privileges. A user with this role can view the system configuration but cannot modify it. |
|  | *Help Desk* – Indicates help desk privileges. A help desk user is allowed to use troubleshooting tools like sniffers, execute service commands, view or retrieve logs. However, help desk personnel *are not* allowed to conduct controller or service platform reloads. |
|  | *Web User* – Indicates a web user privilege. A Web user is allowed accessing the device's Web UI. |

## Device Icons

The following icons represent the different device types managed by the system:

| | |
|---|---|
|  | *System* – This icon represents the entire WiNG supported system, and all of its member controller, service platform or access points that may be interacting at any one time. |
|  | *Cluster* – This icon represents a cluster. A cluster is a set of wireless controllers or service platforms working collectively to provide redundancy and load sharing amongst its members. |
|  | *Service Platform* – This icon indicates an NX 5500, NX 7500, NX 9500 or NX 9600 series service platform that's part of the managed network |
|  | *Wireless Controller* – This icon indicates a wireless controller that's not part of the managed network. |
|  | *Wireless Controller* – This icon indicates a wireless controller that's part of the managed network. |
|  | *Access Point* – This icon lists any access point that's part of the managed network. |
|  | *Wireless Client* – This icon defines any wireless client connection within the network. |

# 4 Quick Start

## Using the Initial Setup Wizard

WiNG access points utilize an initial setup wizard to streamline getting on the network for the first time. This wizard configures location, network and WLAN settings and assists in the discovery of access points and their connected clients.

## Using the Initial Setup Wizard

This chapter describes how to use the **Initial Setup Wizard** to bring up an *access point* (AP), with minimal configurations, to access the wireless network. When bringing up an AP for the first time, use the wizard to define the AP's basic, required settings, such as operational mode, deployment location, basic security, network and WLAN settings. Once the AP is up and running, use the AP's GUI to configure the remaining, advanced, user-interface functionalities.

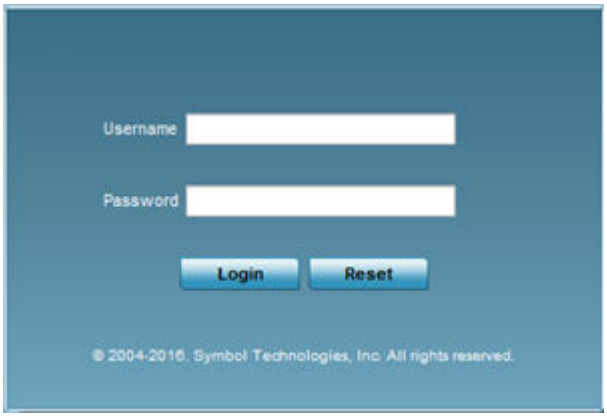
To bring up an AP for the first time, follow the steps below:

1 Install and power up the AP.

For more information, see Connecting to Web UI on page 18.

2 Point the Web browser to the AP's IP address.

The AP's Web UI login screen displays.

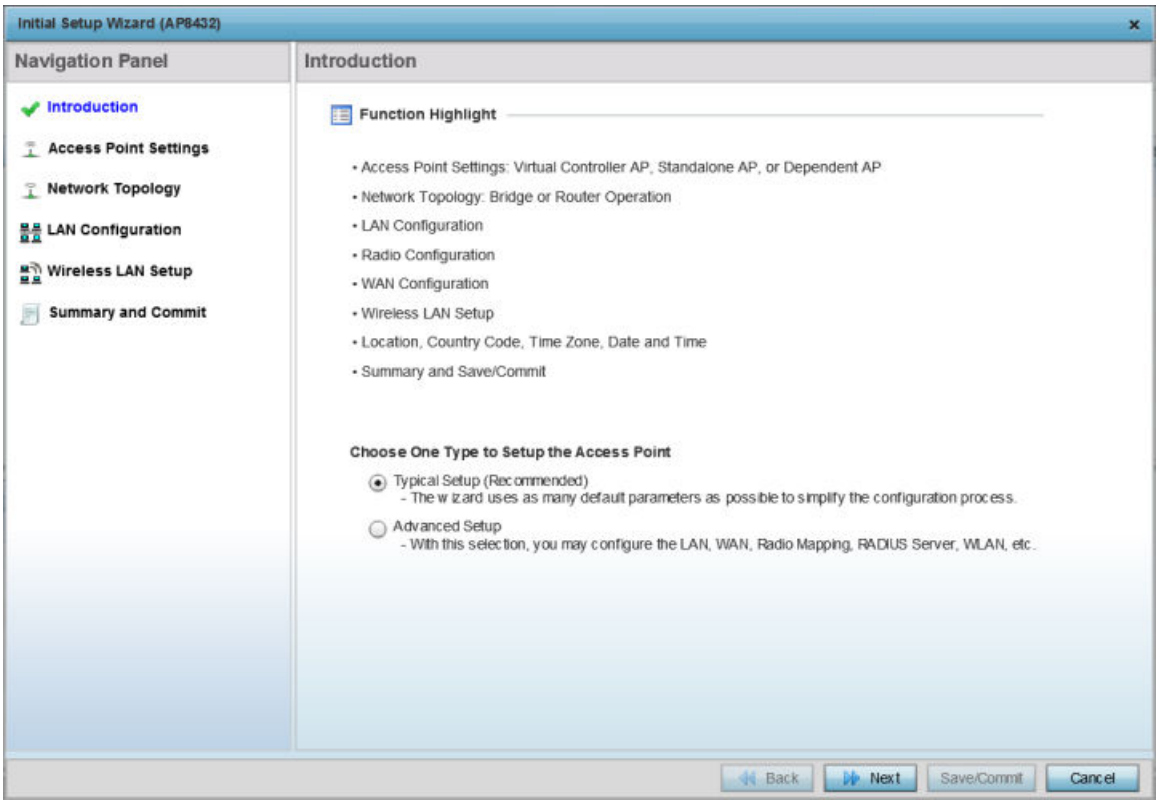



3 Enter the default user name `admin` in the **User name** field.

4 Enter the default password `admin123` in the **Password** field.

**Note**
When logging in for the first time, you will be prompted to change the password. Set a new password and use it for subsequent logins.

The AP's management interface UI displays, and the **Initial Setup Wizard** landing page pops up.




**Note**
The **Initial Setup Wizard** displays the same pages and content for all the WiNG AP model types – the only difference being the number of radios supported on the AP.

The landing page has the following elements:

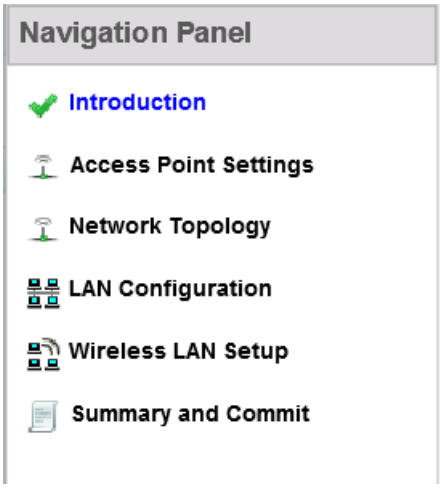
| | |
|---|---|
| **Introduction:** | Lists the tasks you can perform using this wizard. |
| **Navigation Panel:** | Provides links to configuration pages where you can perform the tasks listed in the **Introduction** pane. |
| **Choose One Type to Setup the Access Point** | Provides two AP setup wizards. The options are: **`Typical Setup`** and **`Advanced Setup`**. The links available on the **Navigation Panel** vary depending on the option you select. |

Selecting the Access Point Setup Wizard Type.

5 Select one of the following AP setup wizards:

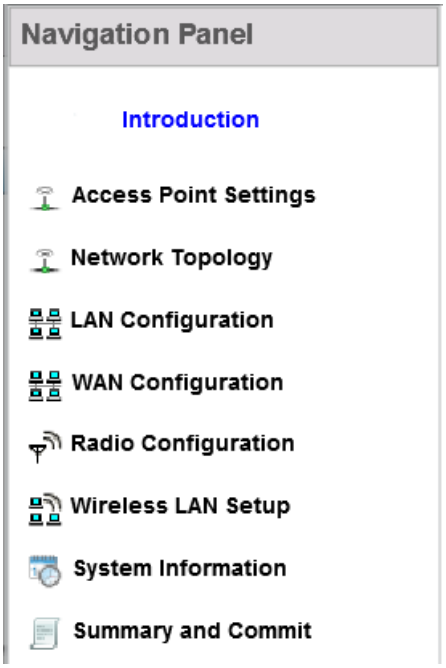
- **Typical Setup** - Select this option to apply system-provided, default values on the AP. We recommend using this option because it simplifies the configuration process. This option is enabled by default.

  The **Typical Setup → Navigation Panel** lists the following configurable features:




- **Advanced Setup** - Select this option to configure user-specific values instead of applying default settings. This option provides additional configurable features, such as **`Radio Configuration`**, **`System Information`**, and **`WAN Configuration`**.

  The **Advanced Setup** → **Navigation Panel** lists the following configurable features:




A green check-mark to the left of a task, on the Navigation Panel, indicates that the minimum required configurations for that task have been set correctly. It is mandatory to have each task green check-marked to successfully complete the initial setup.

A red X against a task indicates that at least one mandatory parameter is pending configuration.

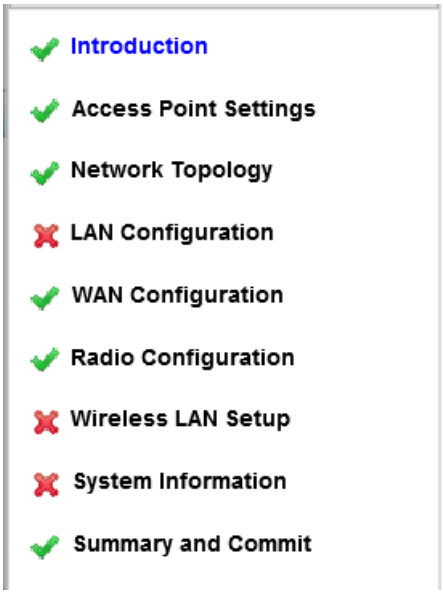



**Figure 3: Red, Green Check-marks**

6 Select the **Summary and Commit** link, on the Navigation Panel, to view and commit your changes.

7 Select **Next** to proceed to the next page.

Select **Back** to revert to the previous page without saving your updates.

Select **Cancel** to close the wizard without committing your changes.

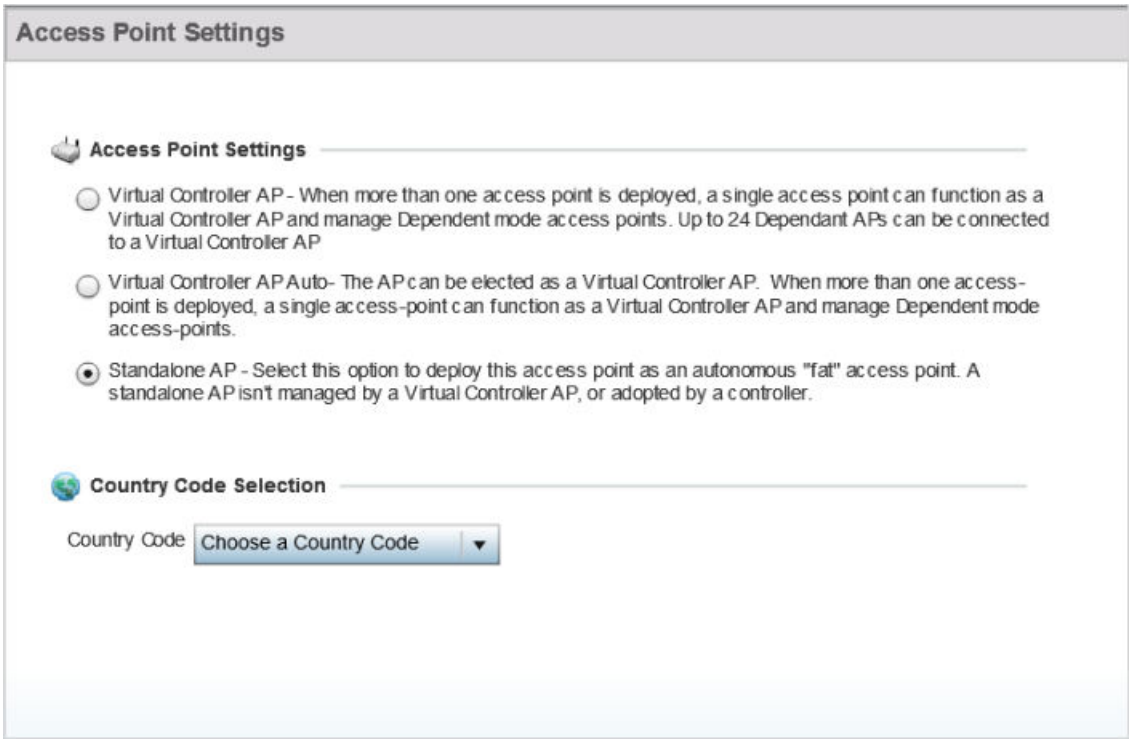
Select **Save/Commit** to save changes made to a page. We recommend that you save your updates before moving to the next page.

Tasks Common to both Wizard Types.

The following steps describe tasks that are common to both wizards.

8 Click **Next**.

The Access Point Settings page displays. Use this page to specify the AP's mode of functioning.




Configuring the Access Point Settings.

9 Set the AP's mode of functioning as one of the following:

- **Virtual Controller AP** - Select to configure the AP to function as a *virtual controller* (VC). In a multiple-AP network, you can configure one of the APs as the VC. For information on the adoption capabilities of the different WiNG AP model types, see Heterogeneous AP Management on page 9.
- **Virtual Controller AP Auto** - Select to enable *dynamic virtual controller* (DVC) mode on the AP. When enabled, the AP on being elected as the RF Domain manager takes on the role of the VC. If you have deployed multiple APs in an RF Domain, you can enable DVC on more than one AP. However, only the current RF Domain manager AP has a running instance of the DVC.

  If enabling DVC, configure the AP's management interface settings:


  - Use the **Virtual Controller Management VLAN** spinner control to set the management interface's *virtual local area network* (VLAN). This VLAN is exclusively used by the VC to broadcast MiNT packets, and to adopt APs. The default setting is VLAN 1.
  - Enter the management interface IP address and subnet in the **Virtual Controller Management Interface IP** field.

Because of the random nature of DVC, specifying an explicit management interface IP address makes it easier to manage VCs. In case of failover, this IP address is installed as the secondary IP address on the new VC.

Configuring a management interface IP address is mandatory. However, VLAN configuration is optional. If you configure the IP address without specifying the VLAN, the system sets the specified IP address as secondary IP on VLAN 1.

- **Standalone AP** - Select to deploy the AP as an *independent* AP, not managed by a VC, or adopted by a wireless controller/service platform. .

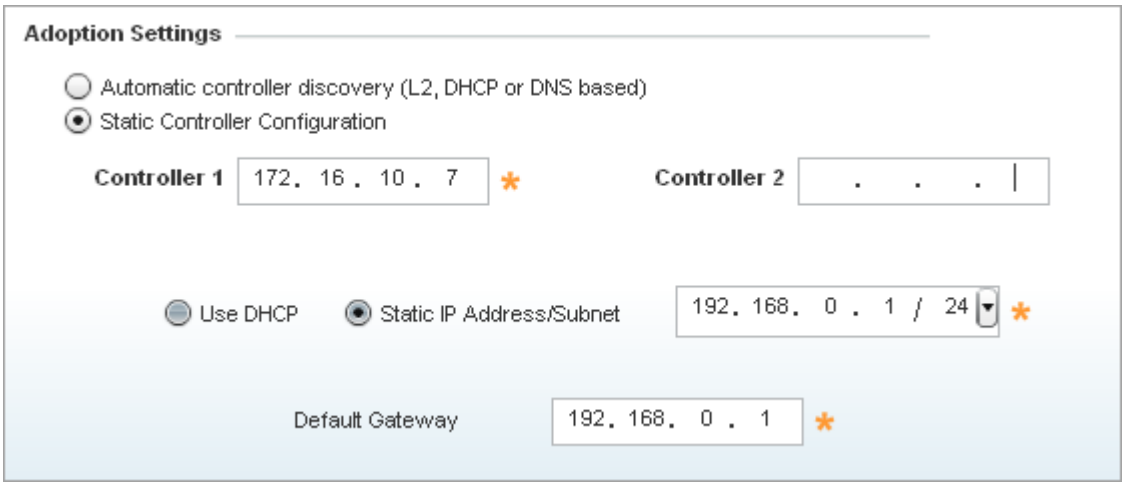
Note
If designating the AP as a Standalone AP, exclusively use the AP's UI, and not the CLI, to configure the AP's settings. The CLI allows you to define more than one profile, whereas the UI does not. Consequently, you might encounter problems if using both interfaces to manage profiles.

- **Adopted to Controller** - Select to deploy the AP as a controller-managed, dependent AP.

Note
The **Adopted to Controller** option is available only on the **Advanced Setup** wizard.

Note
A controller-adopted AP obtains its configuration from a profile stored on its managing controller. Manual changes made on the AP are overwritten by the controller upon reboot.

If enabling controller adoption, configure the following Adoption Settings:




- Select **Automatic controller discovery (L2, DHCP or DNS based)** to enable dynamic discovery and adoption of the AP by any controller within the same subnet. The AP is *Layer 2* (L2) adopted to the controller.
- Select **Static Controller Configuration** to manually configure the controller to which the AP should adopt. This is applicable only in case of *Layer 3* (L3) adoption.

If enabling L3 adoption:

Enter the IP address of the primary controller in the **Controller 1** field.

Enter the IP address of the secondary controller in the **Controller 2** field.

When configured, the AP tries to adopt to Controller 1 first. If the controller is unreachable, the AP tries to adopt to Controller 2.

Select **Use DHCP** to enable dynamic network address assignment. If selected, the AP's IP address is provided by the local DHCP server resource.

Alternately, select the **Static IP Address/Subnet** option to manually configure the AP's network address.

Enter the **Default Gateway** IP address to enable the AP to forward traffic destined for other networks.

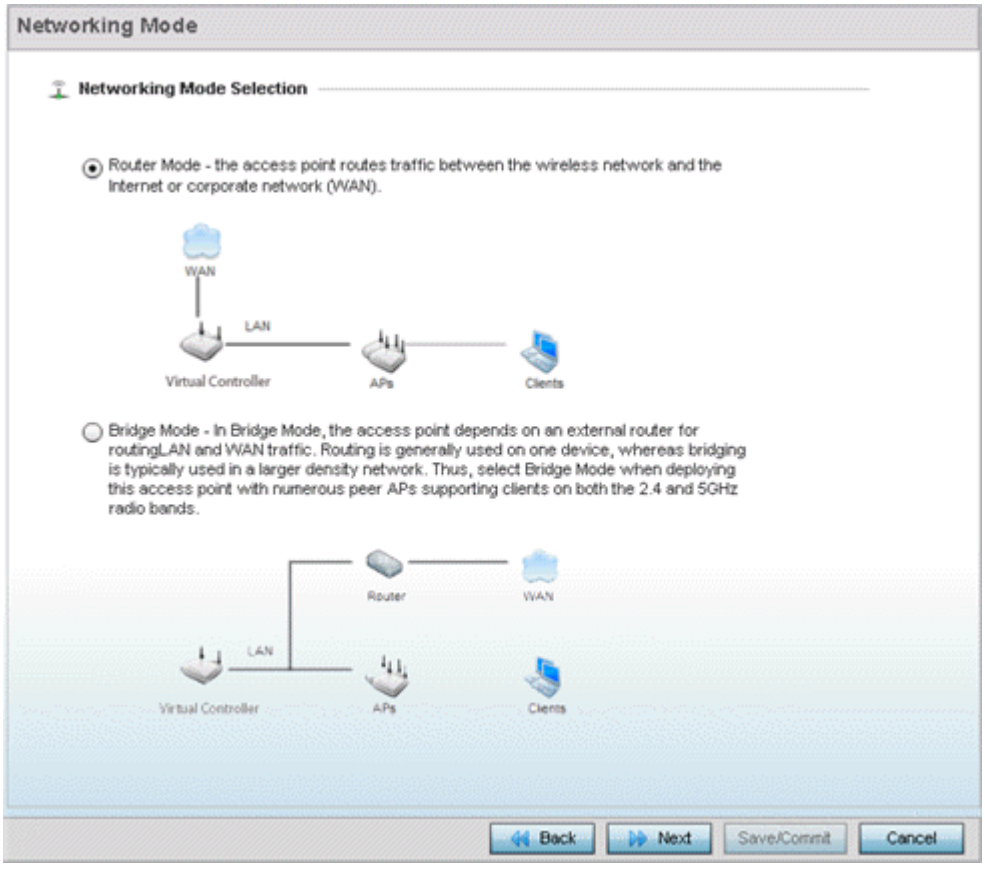
10 Use the **Country Code Selection** spinner control to set the AP's country of deployment.

Ensure that the country code is set correctly because parameters – for example, the available channels of operation and regulatory compliance rules – are country specific.

This option is available only on the Typical Setup wizard.

11 Select **Next**.

The Networking Mode page displays. Use this page to define the AP's network-traffic handling mode.




Configuring the AP's Network Topology Settings.

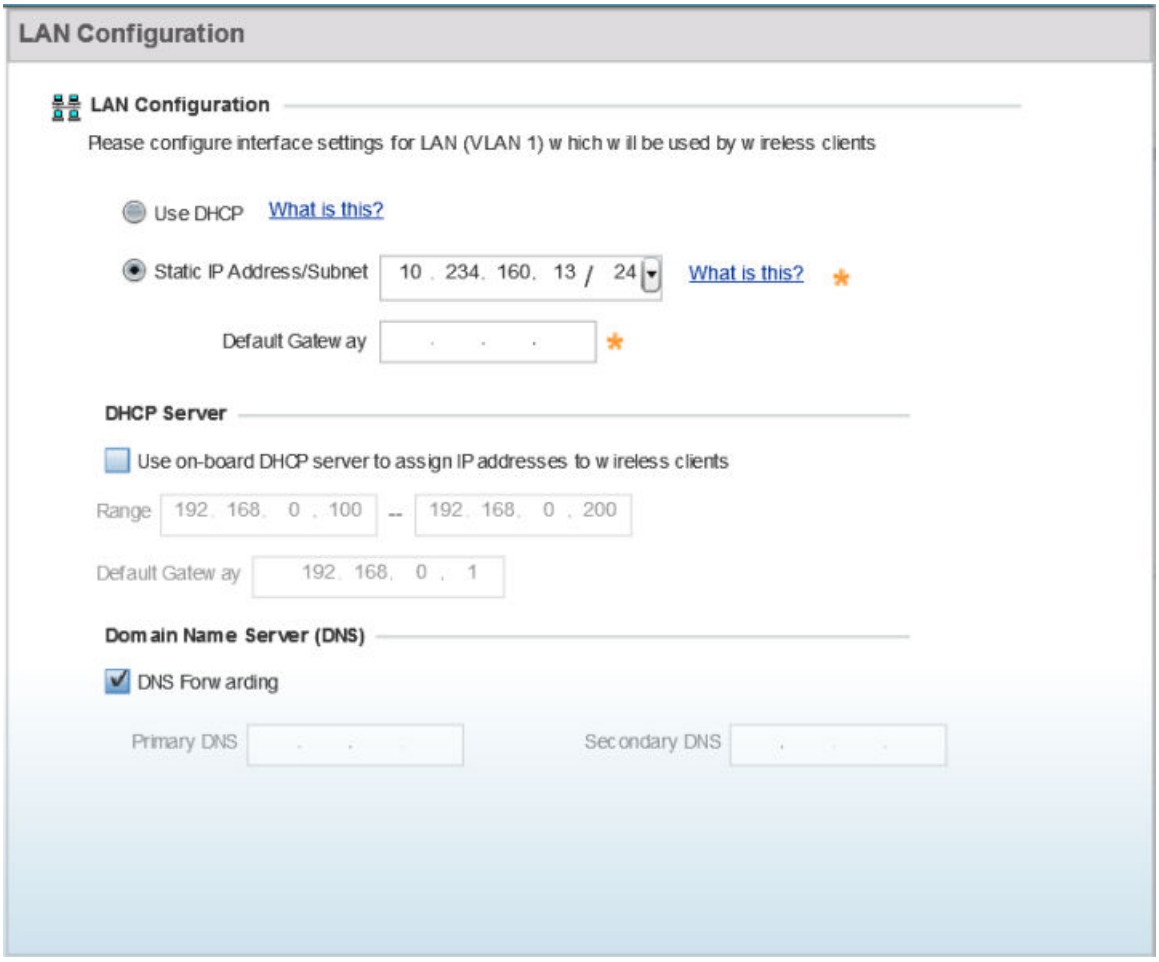
12 Set the AP's Networking Mode Selection as:

- **Router Mode** - Select to enable the AP to function as a router. When enabled, the AP routes traffic between the *local area network* (LAN) and the Internet or external *wide area network* (WAN). We recommend using this option in single-AP supported deployments.
- **Bridge Mode** - Select to enable the AP function as a bridge between the LAN and the Internet or WAN. When enabled, the AP uses an external router to bridge traffic. We recommend using this option in multiple-AP deployments, with APs supporting clients on both the 2.4 GHz and 5.0 GHz radio bands.

Note
The **Bridge Mode** does not require WAN configurations on the AP. Therefore, if you select this option, the WAN configuration option is disabled.

13 Select **Next**.

The LAN Configuration screen displays. Use this screen to configure the AP's LAN address, DHCP server, and DNS server.




Configuring the AP's LAN Settings.

14 Select one of the following options to configure the IP address of the AP's LAN interface:

- **Use DHCP** - Select to enable dynamic IP address assignment. When selected, the local DHCP server resource, running on VLAN 1 (the default VLAN), assigns the IP address.

  Note
  If you select this option, the AP's VLAN 1 (the default VLAN interface of the AP) is dynamically assigned an IP address by the DHCP server running on VLAN 1. Therefore, if you select this option, ensure that a DHCP server is up and running on VLAN 1 and is reachable from the AP.

- **Static IP Address/Subnet** - Select to manually configure the AP's IP address and subnet.
  - Enter the AP's LAN interface IP address and subnet in the **Static IP Address/Subnet** field.
  - Enter the default gateway's IP address in the **Default Gateway** field.

    Note
    The AP routes inter-VLAN traffic through the default gateway.

Note
If you configure a static IP and subnet for the AP, also enable it to function as an on-board DHCP. Therefore, if you select this option, configure the DHCP server and DNS server settings. For DHCP server configurations, move to step 15. For DNS server configurations, move to step 16.

15 Set the following **DHCP Server** settings:

a Select the **Use on-board DHCP server to assign IP addresses to wireless clients** option to enable the AP to function as the on-board DHCP server resource.

When this option is enabled, the AP provides its IP address to requesting wireless clients on the LAN interface.

b Enter the starting and ending IP addresses in the **Range** fields.

The AP assigns IP addresses to authenticated wireless clients from the specified range.

Avoid assigning IP addresses from x.x.x.1 - x.x.x.10 and x.x.x.255, as they are often reserved for standard network services.

c Enter the IP address of the default gateway, in the **Default Gateway** field.

16 Select one of the following options to configure the **Domain Name Server** :

- Select the **DNS Forwarding** option to enable DNS forwarding on the AP. This option is enabled by default.

  DNS forwarding is useful when a request for a domain name is made, but the DNS server responsible for resolving the name into its corresponding IP address cannot locate the matching IP address.

  Note
  Disabling **DNS Forwarding** enables the **Primary DNS** and **Secondary DNS** fields.

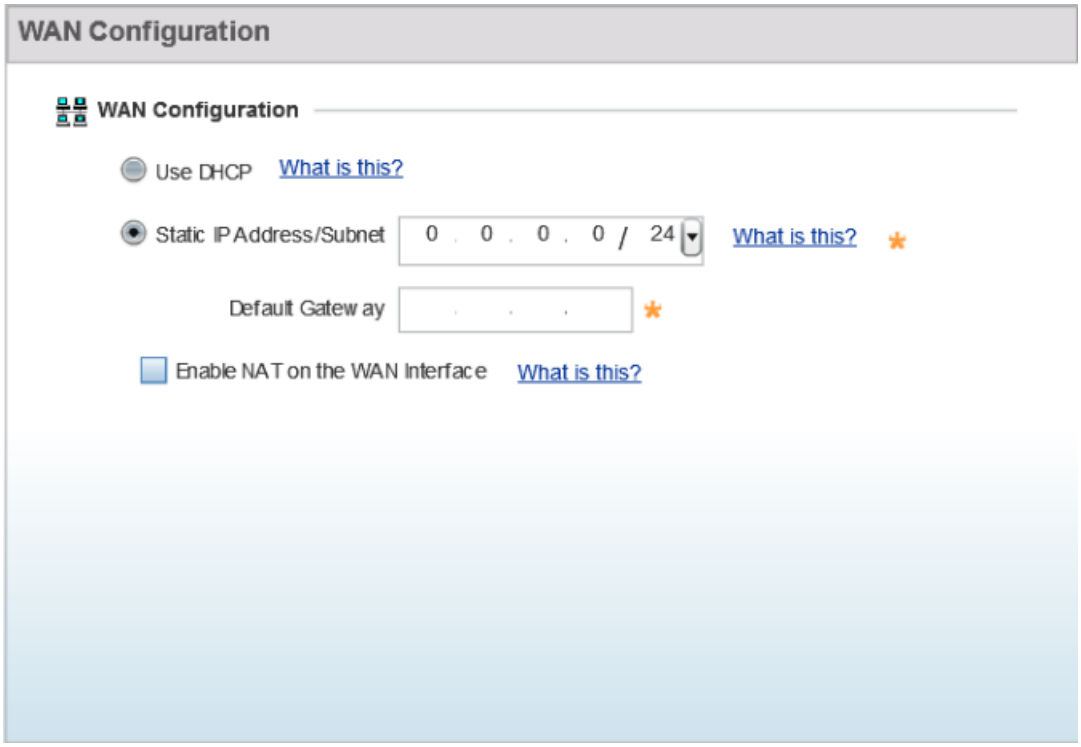
- Configure the following external DNS server resource parameters:
  - Enter the **Primary DNS** server resource IP address. When specified, the AP forwards DNS resolution requests to the specified resource.
  - Enter the **Secondary DNS** server resource IP address.

Configuring the AP's WAN settings.

17 Select **Next**.

The WAN Configuration page displays. Use this page to define network address settings for the AP's WAN interface. The WAN interface connects the AP to the wired local area network or backhaul.

Note
The WAN Configuration option is enabled only if you set the AP in **Router Mode** on the Networking Mode page (see step 11 ).



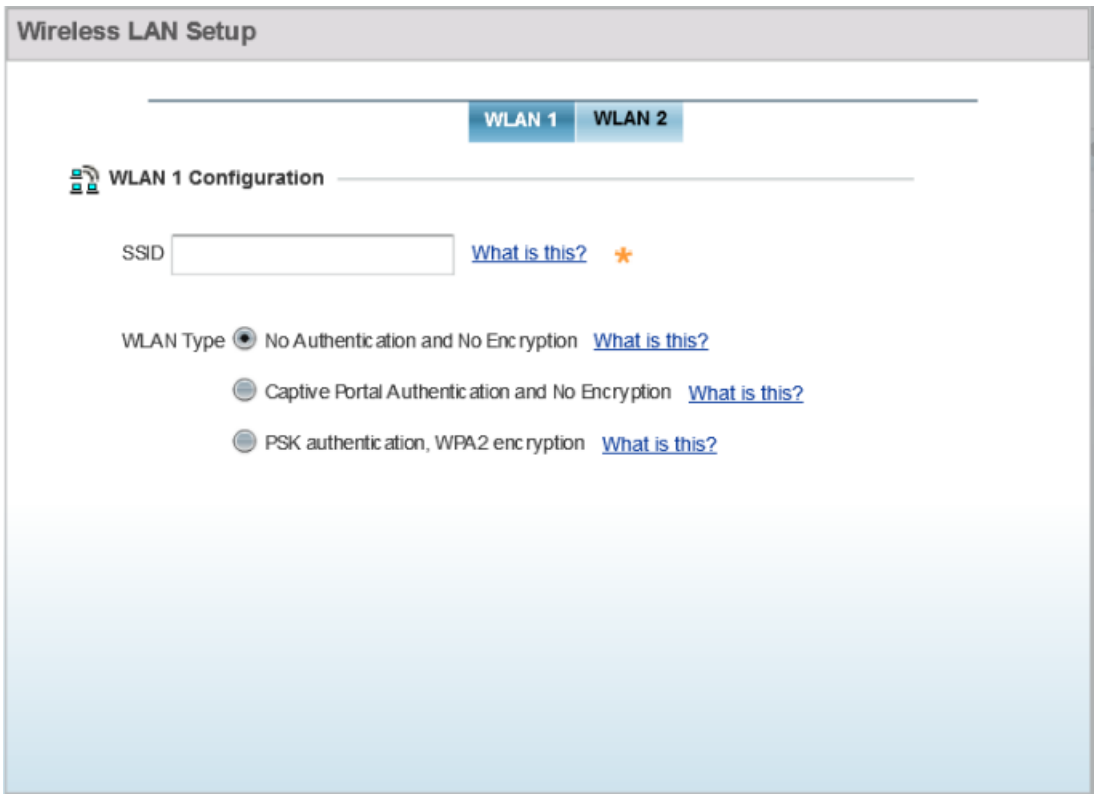
18 Select one of the following options to configure the AP's WAN interface's IP address:

- **Use DHCP** - Select to enable dynamic IP address assignment. When selected, an external DHCP server resource, located on the WAN side of the network, assigns an IP address to the AP's WAN interface.
- **Static IP Address/Subnet** - Select to manually configure IP address and subnet for the AP's WAN interface.
  - Enter the AP's WAN interface IP address and subnet in the **Static IP Address/Subnet** field.
  - Enter the default gateway's IP address in the **Default Gateway** field.

    The Default Gateway is a router that serves as the gateway to other networks.

19 Select **Next**.

The Wireless LAN Setup page displays. Use this page to configure the AP's *Wireless Local Area Network* (WLAN) settings.




A WLAN is a means of flexibly extending the functionality of a *wired LAN*. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus desirable for wireless networking. Roaming users can be handed off from one AP to another, as with a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

Configuring the WLAN Settings.

Note

You can configure up to two (2) WLANs for the AP.

20 Set the following WLAN parameters:

a Enter the WLAN's **SSID**.

b Select the **WLAN Type**.

The WLAN Type defines the encryption and authentication modes used with the WLAN.

- **No Authentication and No Encryption** – Select to configure a network without any authentication or encryption.

> **Note**
> When selected, any device can access the network. Data transmitted through the network is in plain text.

- **Captive Portal Authentication and No Encryption** – Select to configure a network using Captive Portal (Web page) based authentication.

> **Note**
> When selected, the network serves a Web page (internally or externally hosted) to wireless clients requesting network access. The clients enter their login credentials on this Web page. These credentials are authenticated by a RADIUS server. On successful authentication clients are granted access. Once on the network, the data transmitted through the network is in plain text.

> **Note**
> If selecting this option, move to step 21 to configure the RADIUS server details.

- **PSK authentication, WPA2 encryption** – Select to configure a network that uses PSK authentication and WPA2 encryption.

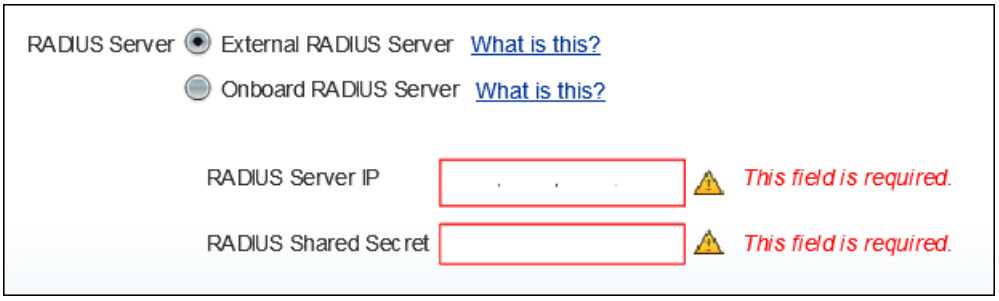
> **Note**
> When selected, wireless clients are granted network access only if the *pre-shared key* (PSK) configured on the AP matches the PSK configured on the client.

> **Note**
> If selecting this option, move to step 22 to configure the PSK.

Configuring RADIUS server for the *Captive Portal Authentication and No Encryption* network.

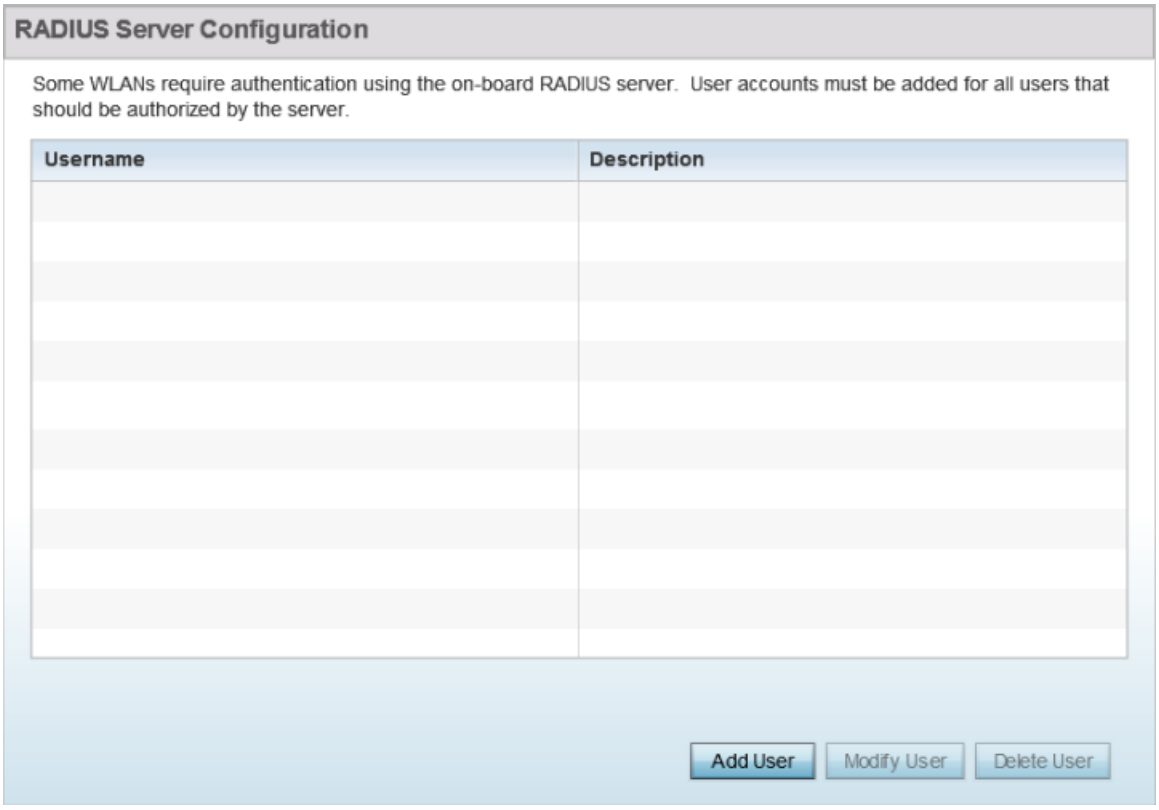
21 Specify the RADIUS Server type as one of the following:

- **External RADIUS Server** - Select to use an externally hosted RADIUS server for user authentication. This is the default setting.

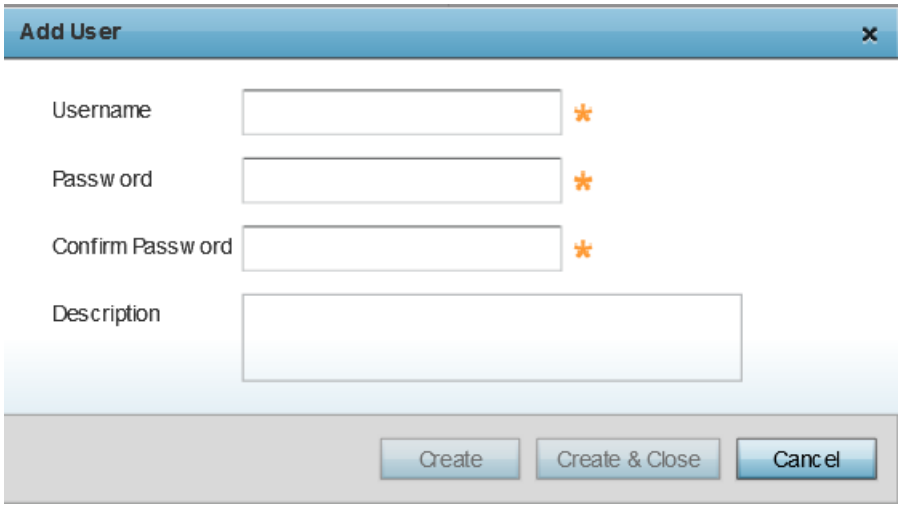


- Enter the external RADIUS server resource IP address in the **RADIUS Server IP** address field.
- Enter the shared secret needed to access the RADIUS server, in the **RADIUS Shared Secret** field.

- **Onboard RADIUS Server** – Select to configure the AP as the RADIUS server that performs user authentication. A RADIUS Server Configuration window is displayed, where you add users to the RADIUS server database.




- Click **Add User** to add a new user. The Add User dialog displays.




| | |
|---|---|
| User name | Enter the client's user name. |

| | |
|---|---|
| Password | Enter the password associated with the specified user name. |
| Confirm Password | Re-enter the password. |
| Description | Enter a short description for the user. |

- Click **Create** to add the new user and continue adding other users.
- Click **Create & Close** to add the new user and close the dialog.
- To modify an existing user in the RADIUS server database, select the user from those listed and click **Modify User**. In the Modify User dialog, make the required changes and click **Modify User**.

Note
You cannot modify the Username. However, Password and Description can be modified.

- To delete an existing user in the RADIUS server database, select the user from those listed and click **Delete User**. A confirmation dialog displays. Click **Yes** to confirm deletion.

Configuring PSK for the PSK authentication, WPA2 encryption network.

22 To specify the PSK needed for client authentication:

a Use the drop-down menu to specify the PSK type as ASCII or HEX.

b Enter the PSK in the **WPA Key** field.

Provide a 64-character HEX key or an 8-63 character ASCII key, based on the PSK type you have selected.

Advanced Setup-specific Tasks.

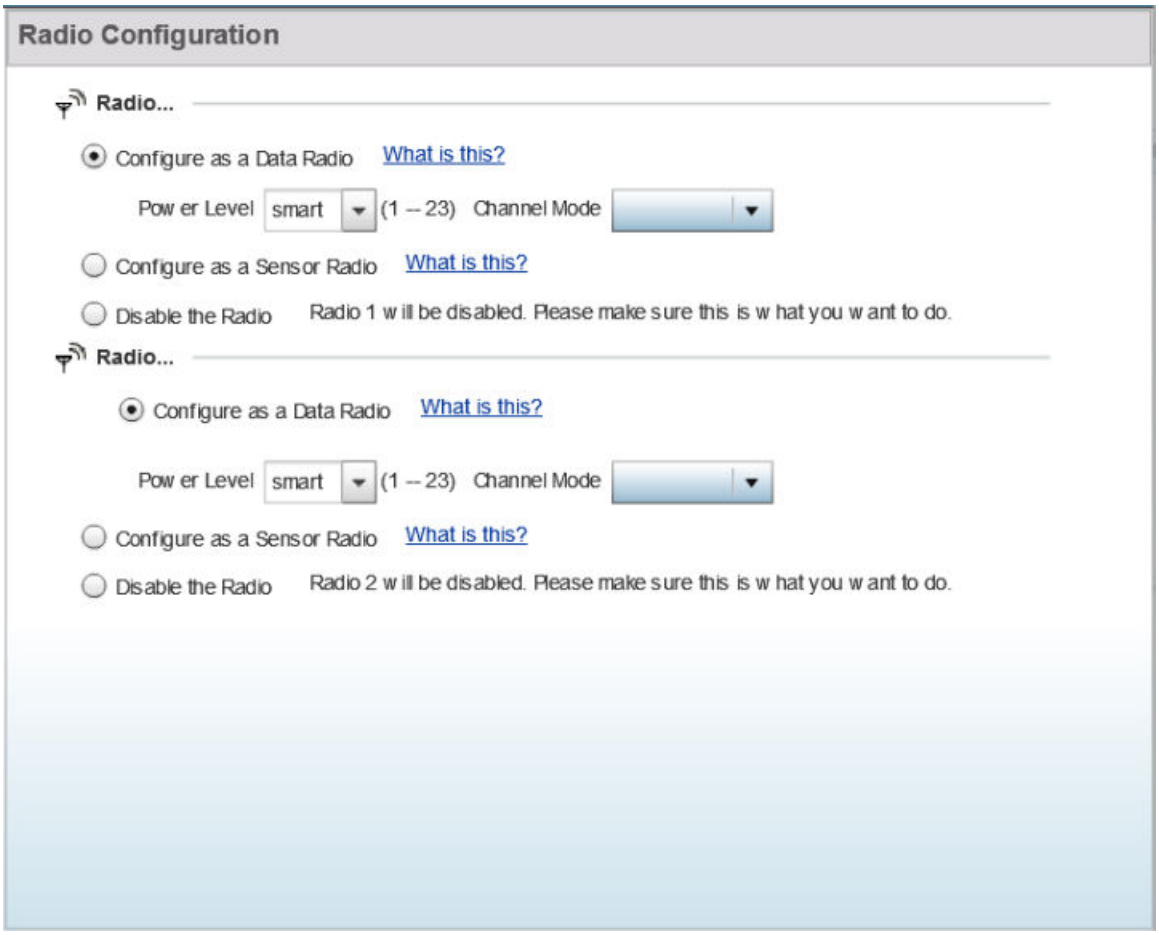
The following steps describe the tasks specific to the **Advanced Setup** wizard.

23 Click **Next**.

The Radio Configuration page displays. Use this page to set the radio's mode of operation. The radio can be set to transmit data to and from wireless clients, or it can be configured to function as a dedicated sensor.

**Note**
The number of configurable radios displayed depends on the AP's model type.

The following image shows an AP with two radios:




Configuring the AP's Radio Interface.

24 Set the following parameters for each radio:

a **Configure as a Data Radio** - Select to dedicate the radio to WLAN client support in the 2.4 GHz or 5.0 GHz radio bands.

b **Power Level** - Use the spinner control to select a 1 - 23 dBm minimum power level to assign to this radio. 1 dBm is the default setting.

c **Channel Mode** - Set the channel selection mode to one of the following:

Random Select to use with 802.11n radios. In the European Union, to comply with *Dynamic Frequency Selection* (DFS) requirements, the 802.11n radio uses a randomly selected channel each time the AP is powered on.

**Best** Select to enable the AP to scan non-overlapping channels and listen for beacons from other APs. After the channels are scanned, the AP selects the channel with the fewest APs. In case of multiple APs on the same channel, it selects the channel with the lowest average power level. Selecting **Best** enables the **Constantly Monitor** option. Select this option to enable the AP to continuously scan the network for excessive noise and sources of interference.

**Static** Select to assign the AP a permanent channel and scan for noise and interference only when initialized.

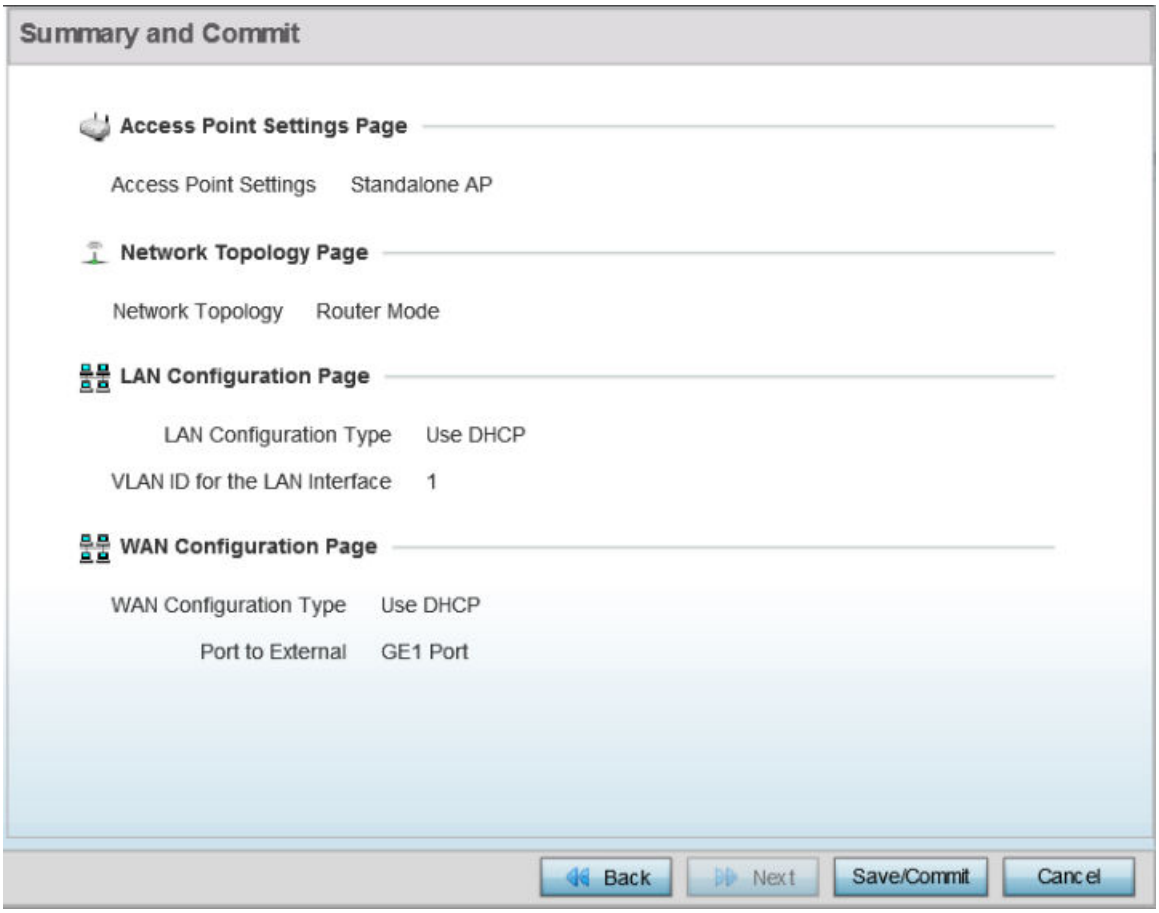
d **Configure as a Sensor Radio** - Select to dedicate the radio to sensor support exclusively. A sensor radio scans all channels within the 2.4 and 5.0 GHz bands to identify potential threats. If you are dedicating the radio to sensor support, also configure a primary and secondary ADSP server, that receives and analyses inputs from the sensor radio.

e **Disable the Radio** - Select to disable the radio. When disabled, the radio goes offline. Verify this course of action with your network administrator before rendering the radio offline.

25 Click **Next**.

The Summary and Commit page displays.

**Note**
This page is available on both the **Typical Setup** and **Advanced Setup** wizards.




Use this page to review and validate the AP's configuration.

- If the AP's configuration warrants additional changes, click **Back**, navigate to the desired page, and make the changes.
- After you have validated the configurations, click **Save/Commit** to apply the changes.

# 5 Dashboard

**Dashboard**

## Dashboard

The dashboard enables administrators to review and troubleshoot network device operation. Additionally, the dashboard allows the review of the network topology, the assessment of the network's component health and a diagnostic review of device performance.

By default, the Dashboard screen displays a Summary of the System dashboard, which is the top level in the device hierarchy. To view information for RF Domains, controllers/service platforms or access points, expand the **System** node and select the desired, associated item in the tree.

### System Dashboard

The dashboard allows network administrators to review and troubleshoot the operation of the devices comprising the access point managed network. Use the dashboard to review the current network topology, assess the network's component health and diagnose problematic device behavior.

By default, the Dashboard screen displays the System Dashboard, which is the top level in the device hierarchy.

The Dashboard provides the following tools and diagnostics:

- System Health on page 42
- System Inventory on page 44

*System Health*

The Health tab displays performance status for managed devices, and includes their RF domain memberships.

To assess system health:

1 Select **Dashboard** → **Summary** → **System**.

The **System** → **Health** tab displays by default.

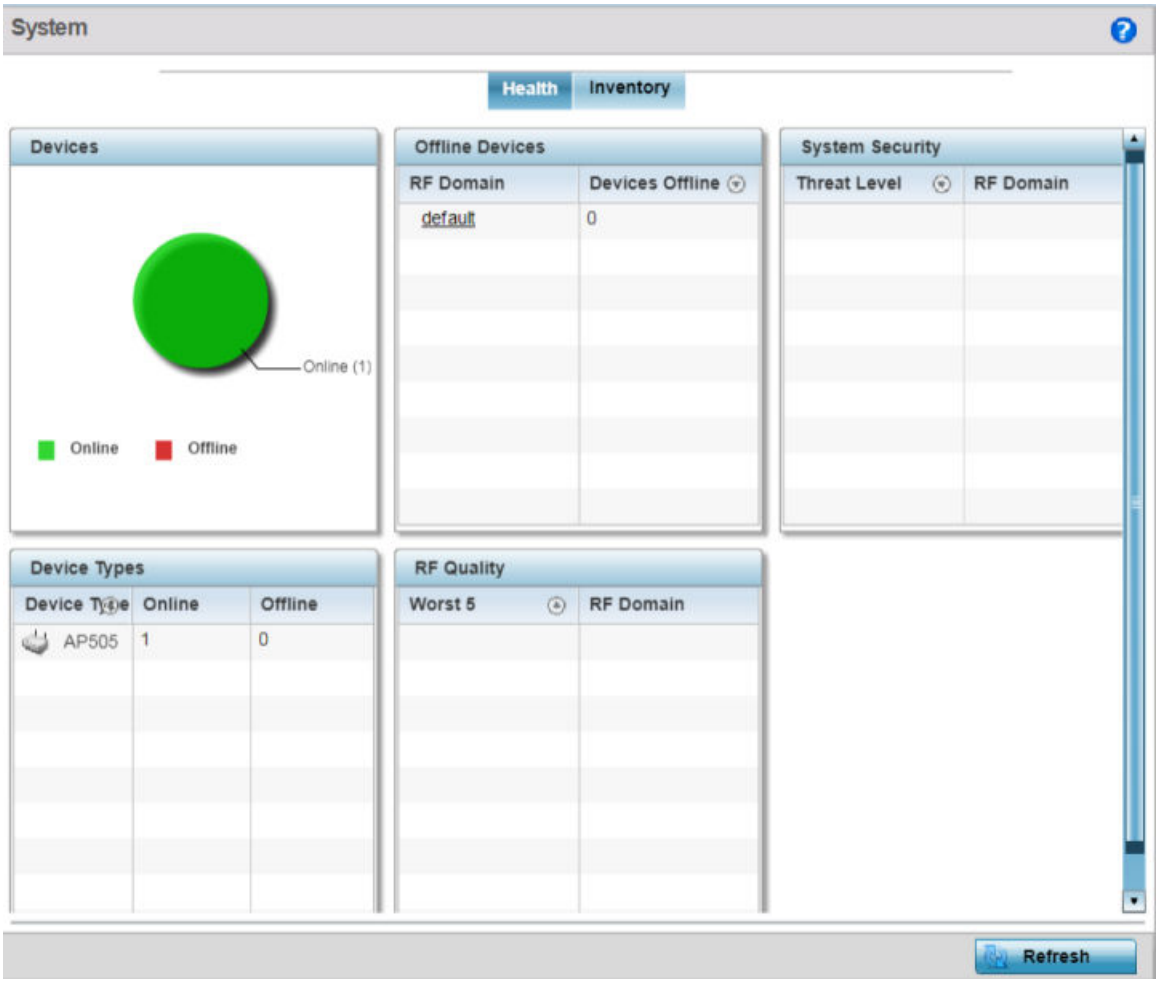



**Figure 4: System - Health Tab**

2 The system health screen is partitioned into the follwoing:

- The **Devices** field displays a ratio of offline versus online devices within the system. The information is displayed in pie chart format to illustrate device support ratios.
- The **Device Types** field displays a numerical representation of the different controller, service platform and access point models in the current system. Their online and offline device connections are also displayed. Does this device distribution adequately support the number and types of access point radios and their client load requirements.
- The **Offline Devices** field displays a table of supported RF domains within the system, with each RF domain listing the number offline devices within that RF domain. Listed RF domains display as individual links that can be selected to RF domain information in greater detail.
- The **RF Quality** field displays RF quality per RF domain. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the connect rate in both directions, retry rate and error rate.
- This field displays an average quality index supporting each RF domain. The table lists the bottom five (5) RF quality values for RF domains. Listed RF domains display as individual links that can be selected to RF domain information in greater detail. Use this diagnostic information to determine what measures can be taken to improve radio performance in respect to wireless client load and the radio bands supported.

  The quality is measured as:
  - 0-20 - Very poor quality
  - 20-40 - Poor quality
  - 40-60 - Average quality
  - 60-100 - Good quality
- The **System Security** field displays RF intrusion prevention stats and their associated threat level. The greater the number of unauthorized devices, the greater the associated threat level. It also displays a list of up to five (5) RF domains in relation to the number of associated wireless clients. The RF domains appear as links that can be selected to display RF domain information in greater detail.

*System Inventory*

The **System** screen's **Inventory** tab displays granular data on specific devices supported within the network. The screen provides a complete overview of the number and state of managed devices. Information is displayed in easy to read tables and graphs. This screen also provides links for more detailed information.

1 Select the **Inventory** tab.

The system inventory screen displays.

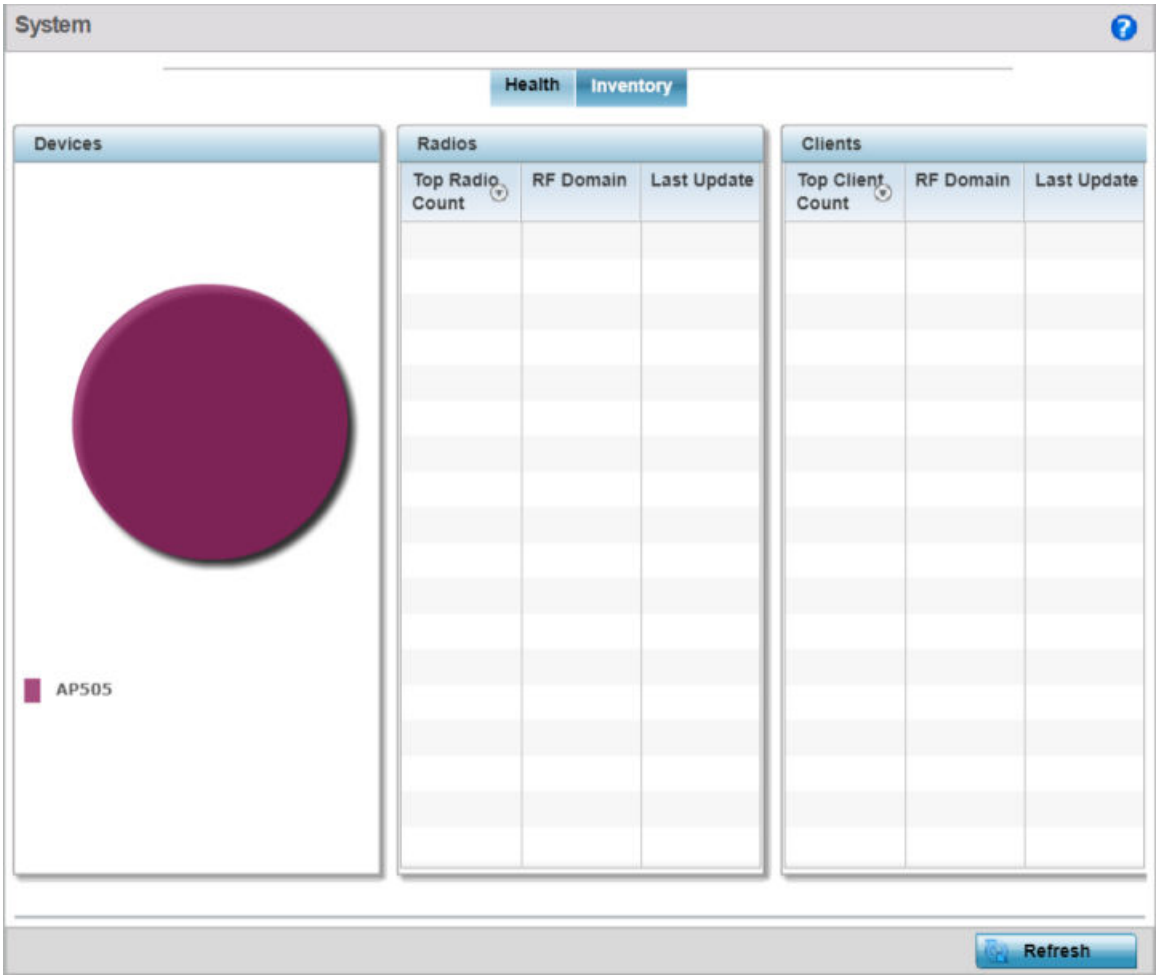



**Figure 5: System Screen - Inventory Tab**

2 Review the following:

The information within the Inventory tab is partitioned into the following fields:

- The Devices field displays a ratio of peer controllers and service platforms as well as their managed access point radios. The information is displayed in pie chart format.
- The Radios field displays top performing radios, their RF Domain memberships, and a status time stamp. RF Domain information can be selected to review RF Domain membership information in greater detail.Information in the Radio area is presented in two tables. The first lists the total number of Radios managed by this system, the second lists the top five RF Domains in terms of the number of available radios.
- The wireless Clients field lists the top five RF Domains with the highest total number of clients managed by connected devices in this system. Select **Refresh** as needed to update the screen to its latest values.

## RF Domain Dashboard

RF domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site. Each RF domain contains policies that can determine a Smart RF or WIPS configuration.RF domains enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of access points servicing the global WLAN. This WLAN override technique eliminates the requirement for defining and managing a large number of individual WLANs and profiles.

A configuration contains (at a minimum) one default RF domain and can optionally use additional user defined RF domains:

The **RF Domain** screen displays system-wide network status. The screen is partitioned into the following tabs:

- RF Domain Health on page 46
- RF Domain Inventory on page 49

### *RF Domain Health*

The RF Domain **Health** tab displays the status of the RF domain's device membership. To assess the RF domain component health:

1 Select **Dashboard** → **Summary**.
2 Expand the **System** node to display RF domains.

3 Select an RF domain.

The RF Domain **Health** tab displays by default.

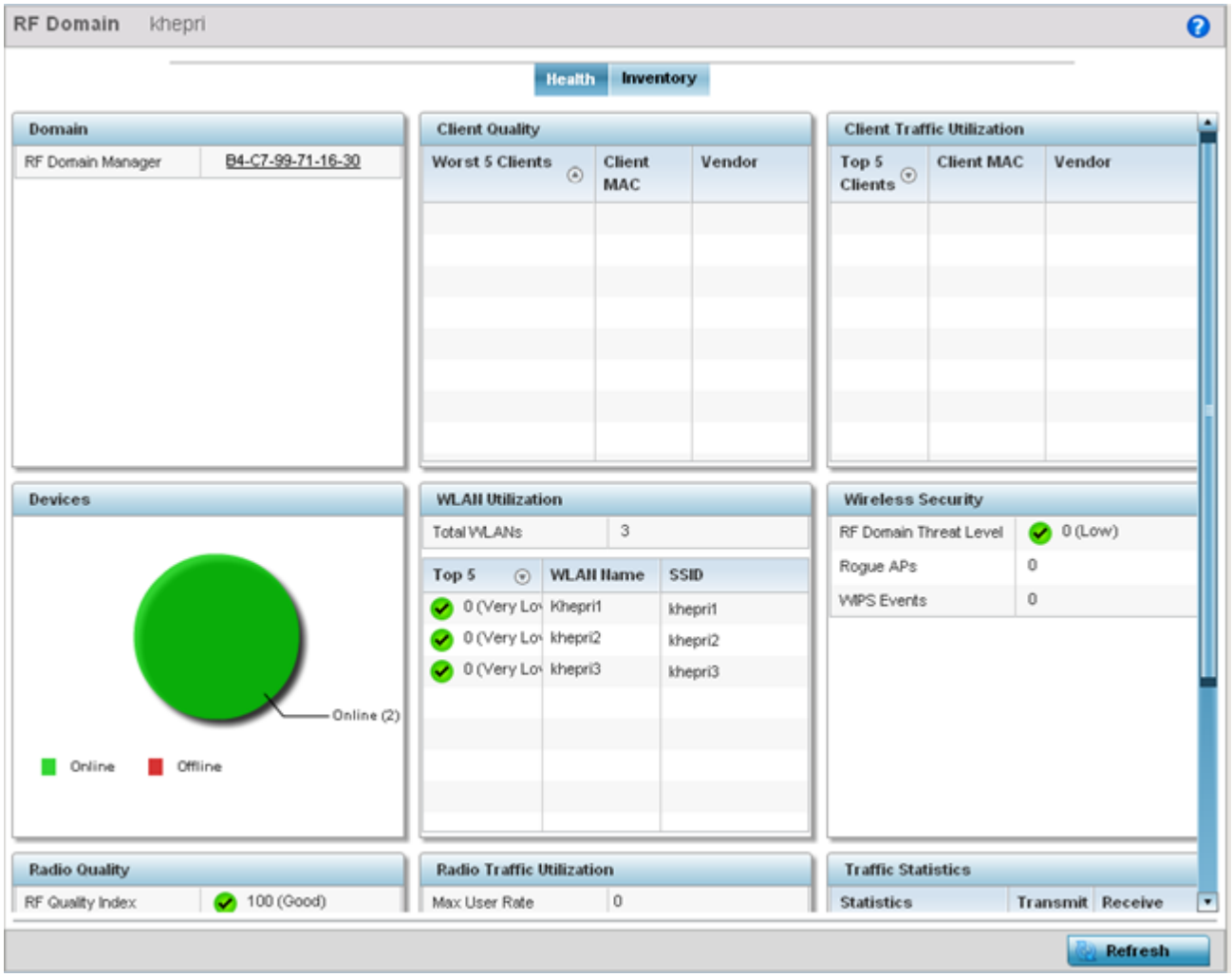



**Figure 6: RF Domain Screen - Health Tab**

4 Refer to the following RF domain health information for member devices:

- The Domain field lists the RF domain manager reporting utilization statistics. The MAC address displays as a link that can be selected to display RF domain information in at more granular level.
- The Devices field displays the total number of devices and the status of the devices in the network as a graph. This area displays the total device count managed by this device and their status (online vs. offline) as a pie graph.

5 The Radio Quality table displays a table of RF quality on a per radio basis. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the transmit retry rate in both directions and the error rate. This area of the screen displays the average quality index across all the defined RF domain on the wireless controller. The table lists worst five of the RF quality values of all the radios defined on the wireless controller. The quality is measured as:

- 0-20 - Very poor quality
- 20-40 - Poor quality
- 40-60 - Average quality
- 60-100 - Good quality

Note
Select a **Radio Id** to view its statistics in greater detail.

6 Refer to the Client Quality table, which displays RF quality for the worst five performing clients. It is a function of the transmit retry rate in both directions and the error rate. This area of the screen displays the average quality index across all the defined RF domain on the wireless controller. The quality is measured as:

- 0-20 - Very poor quality
- 20-40 - Poor quality
- 40-60 - Average quality
- 60-100 - Good quality

Note
Select a **Client** to view its statistics in greater detail.

7 The WLAN Utilization displays how efficiently the WLANs are used. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the WLAN. The total number of WLANs is displayed above the table. The table displays a list of the top five WLANs in terms of overall traffic utilization. It displays the utilization level names, WLAN name and SSIDs for each of the top five WLANs.

8 The Radio Traffic Utilization displays how efficiently the RF medium is used. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the RF domain. The Traffic Index area displays an overall quality level for radio traffic and the Max User Rate displays the maximum data rate of associated radios. The table displays a list of the top five radios in terms of overall traffic utilization quality. It displays the radio names, MAC Addresses and radio types for each of the top five radios.

9 The Client Traffic Utilization displays how efficiently the RF medium is utilized for connected clients. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the clients in the RF domain. The table displays a list of the top five performing clients in respect to overall traffic utilization. It displays the client names, MAC Addresses and vendor for each of the top five clients.

10 The Wireless Security displays the overall threat index for the system. This index is based on the number of Rogue/Unsanctioned APs and *Wireless Intrusion Protection System* (WIPS) events detected. The index is in the range 0 - 5 where 0 indicates there are no detected threats. An index of 5 indicates a large number of intrusion detection events or rogue/unsanctioned APs detected.

11 The Traffic Statistics includes transmit and receive values for Total Bytes, Total Packets, User Data Rate, Broadcast/Multicast Packets, Management Packets, Tx Dropped Packets and Rx Errors.

*RF Domain Inventory*

The Inventory tab displays information on the devices managed by RF domain member devices in the controller, service platform or access point managed network. The Inventory screen enables an administrator to overview of the number and state of the devices in the selected RF domain. Information is displayed in easy to read tables and graphs.

To review the RF domain inventory:

1 Select the **Inventory** tab.

The RF Domain Inventory screen displays.

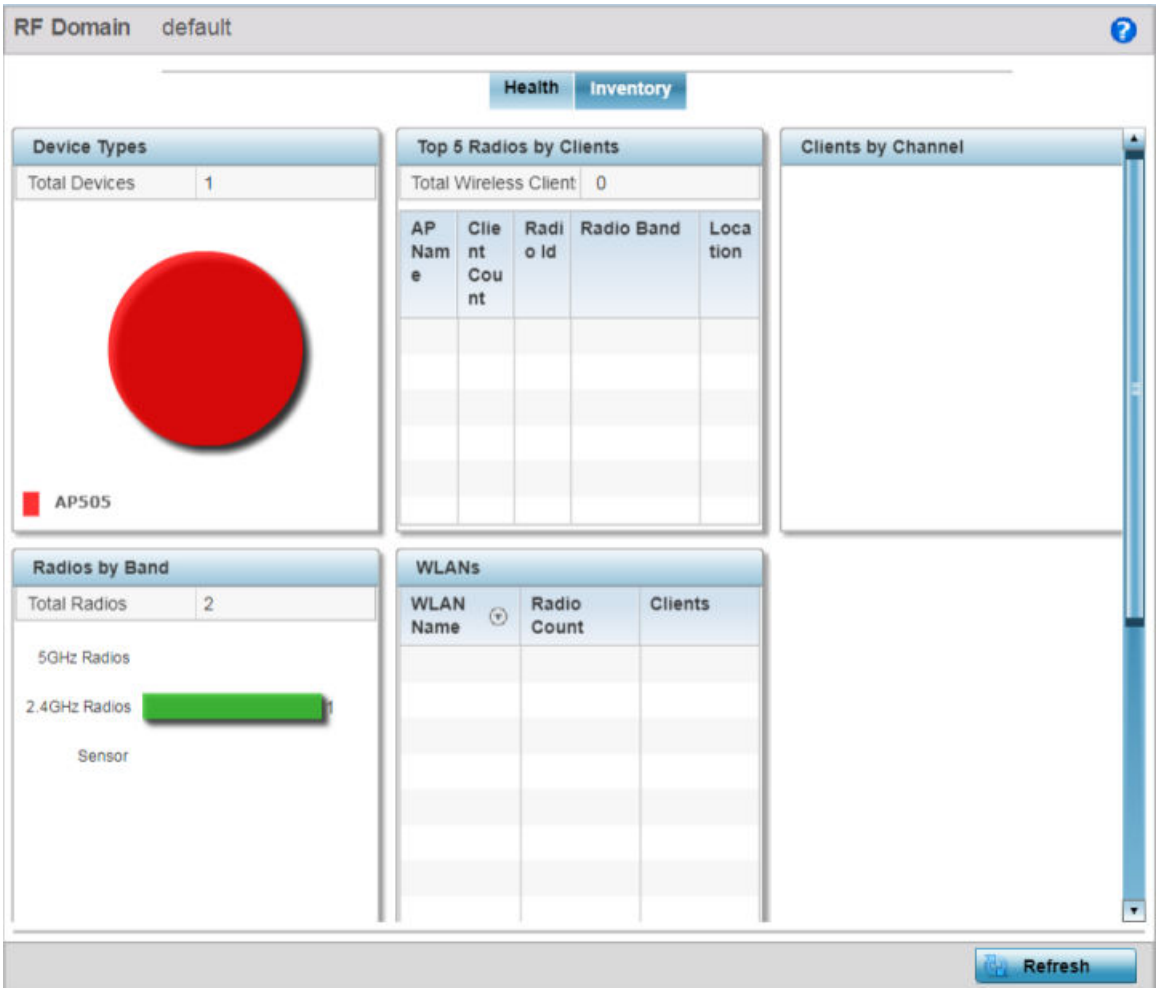



**Figure 7: RF Domain Screen - Inventory Tab**

2 Refer to the following RF domain inventory data collected by member controllers, service platforms or access points:

- The **Device Types** table displays the devices types populating the RF domain. The Device Type area displays an exploded pie chart that displays the type of device and their numbers in the RF domain.
- The **Radios by Band** table displays a bar graph of RF domain member device radios classified by their radio band or sensor dedication. Review this information to assess whether RF domain member radios adequately support client device traffic requirements.
- The **Radios by Channel** table displays pie charts of the different channels utilized by RF domain member radios. These dedicated channels should be as segregated as possible from one another to avoid interference. If too many radios are utilizing a single channel, consider off-loading radios to non utilized channels to improve RF domain performance.
- The **Top 5 Radios by Clients** table displays a list of radios that have the highest number of clients. This list displays the radio IDs as links that can be selected to display individual radio information in greater detail.
- The **WLANs** table displays a list of WLANs utilized by RF domain member devices. The table is ordered by WLAN member device radio count and their number of connected clients. Use this information to assess whether the WLAN is overly populated by radios and clients contributing to congestion.
- The **Clients by Band** table displays the radio band utilization of connected RF domain member clients. Assess whether the client band utilization adequately supports the intended radio deployment objectives of the connected RF domain member access point radios.
- The **Clients by Channels** table displays a bar-graph of wireless clients classified by their frequency. Information for each channel is further classified by their 802.11x band. In the 5GHz channel, information is displayed classified under 802.11a and 802.11an bands. In the 2.4 GHz channel, information is displayed classified under 802.11b, 802.11bg, and 802.11bgn band.

## Access Point Dashboard

The **Access Point** screen displays system-wide network status for standalone or controller-connected access points. The screen is partitioned into the following tabs:

- Access Point Health on page 50 – The **Health** tab displays information about the state of the access point managed network.
- Access Point Inventory on page 53 – The **Inventory** tab displays information on the physical devices managed within the access point managed network.

### *Access Point Health*

To assess access point network health:

1 Select **Dashboard** → **Summary**.
2 Expand the **System** node to display RF domains.

3 Expand an RF domain and select an access point from the list of managed devices.

The selected access point's Health screen displays by default.

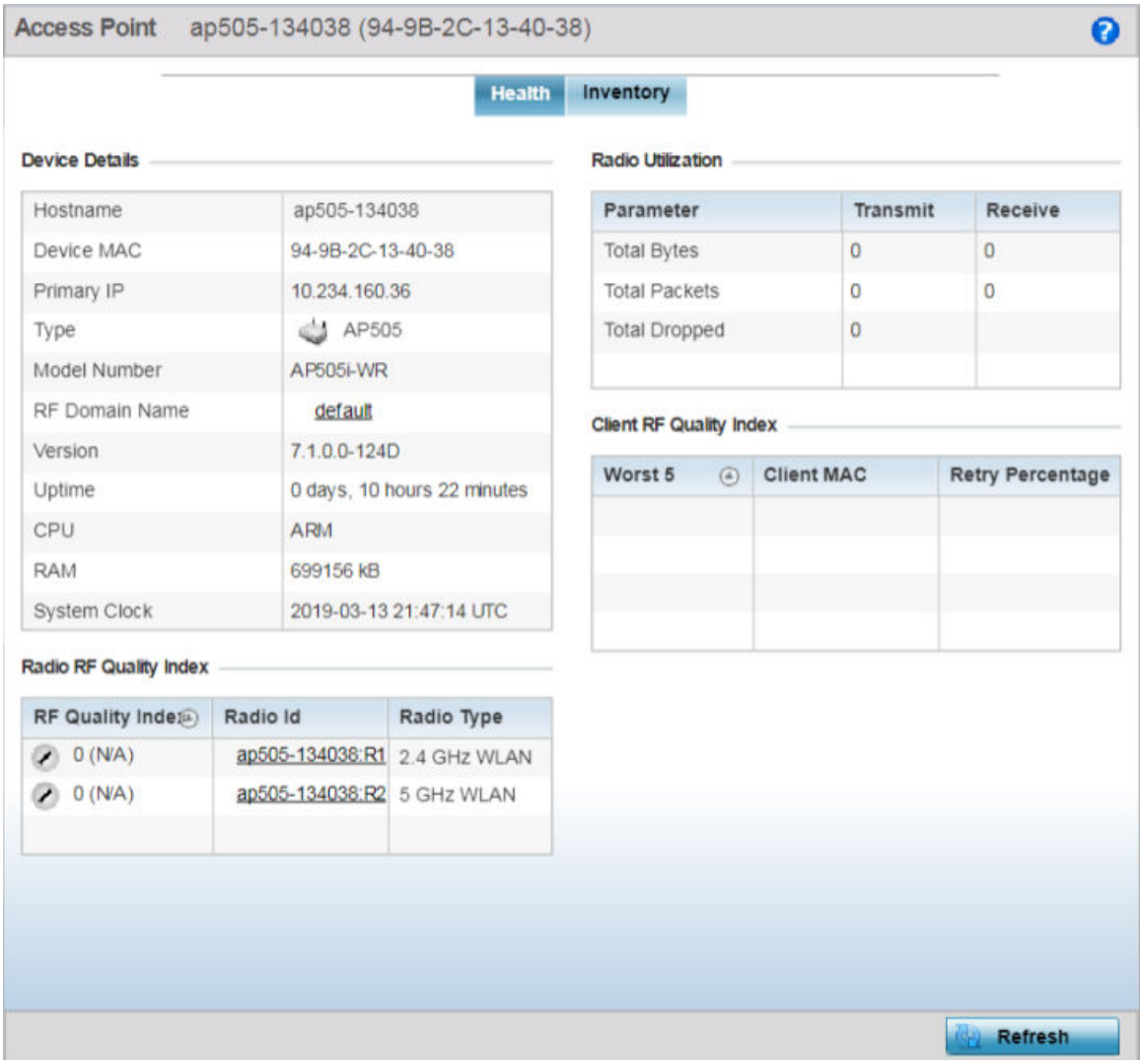



**Figure 8: Access Point Screen - Health Tab**

4 Review the following information:

- Device Details - displays the following information for the selected access point:

| | |
|---|---|
| Hostname | Lists the administrator assigned name of the selected access point. |
| Device MAC | Lists the factory encoded MAC address of the selected access point. |
| Primary IP | Lists the IP address assigned to the access point as a network identifier. |
| Type | Indicates the access point model type. An icon representing the access point is displayed along with the model number. |
| RF Domain Name | Lists the RF Domain to which the access point belongs. The RF Domain displays as a link that can be selected to display access point RF Domain membership data in greater detail. |

| | |
|---|---|
| Model Number | Lists the specific model number of the access point. |
| Version | Lists the version of the firmware running on the access point. Compare this version against the version currently on the support site to ensure the access point has the latest feature set available. |
| Uptime | Displays the duration the access point has been running from the time it was last restarted. |
| CPU | Displays the CPU installed on this access point. |
| RAM | Displays the amount of RAM available for use in this system. |
| System Clock | Displays the current time on the access point. |

- Radio RF Quality Index - displays the bottom five (5) RF quality values for the access point's single default RF Domain. These values are a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the data rate in both directions, the retry rate and error rate. The quality is measured as:
  - 0-20 - Very poor quality

    20-40 - Poor quality
  - 40-60 - Average quality
  - 60-100 - Good quality

  The access point's RF Domain allows an administrator to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site. The RF Domain contains policies that can determine a Smart RF or WIPS configuration. Use this diagnostic information to define measures to improve radio performance in respect to wireless client load and radio band.

  Periodically select **Refresh** (at the bottom of the screen) to update the RF quality data.
- Radio Utilization - field displays how efficiently the RF medium is used by the access point. Radio utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the radio. The Radio Utilization displays radios in terms of the number of associated wireless clients and percentage of utilization. It also lists packets types transmitted and received.

  Refer to the number or errors and dropped packets to assess radio performance relative to the number of packets both transmitted and received.

  Periodically select **Refresh** (at the bottom of the screen) to update the radio utilization information displayed.
- Client RF Quality Index - displays a list of the worst 5 performing clients managed by the selected access point. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the connect rate in both directions, the retry rate and the error rate. The quality is measured as:
  - 0-20 - Very poor quality
  - 20-40 - Poor quality
  - 40-60 - Average quality
  - 60-100 - Good quality

  Periodically select **Refresh** (at the bottom of the screen) to update client RF quality.

*Access Point Inventory*

The access point **Inventory** tab displays granular data on devices managed by the selected access point. Information is displayed in easy to read tables and graphs.

To review the access point's inventory of connected devices:

1 Select the **Inventory** tab.

The selected access point's inventory screen displays.

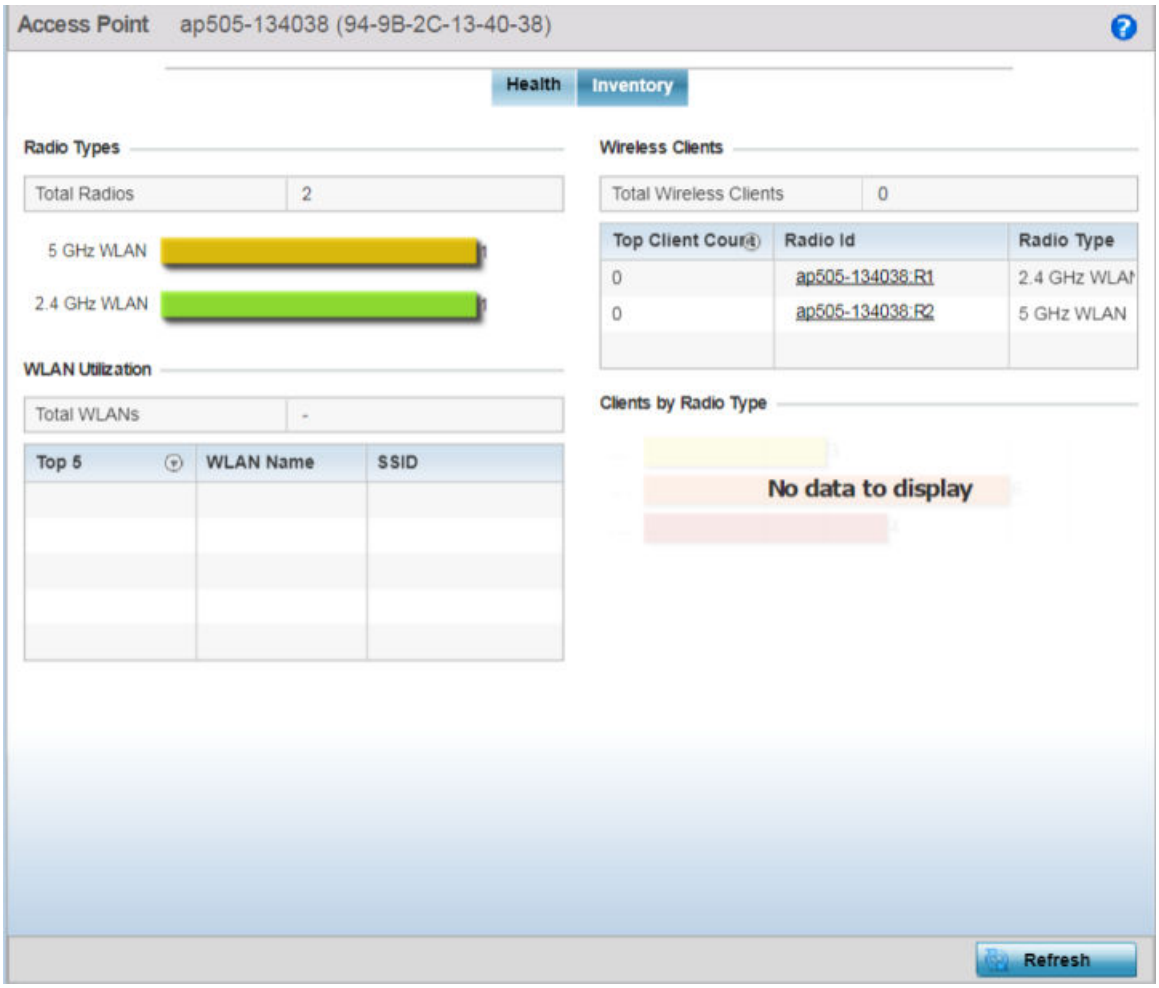



**Figure 9: Access Point Screen - Inventory Tab**

2 Review the following access point invemtory information:

- The Radios Type field displays the total number of radios utilized by this access point. The graph lists the number of radios in both the 2.4 GHz and 5 GHz radio bands. Refer to the Total Radios column to review the number of managed radios. Additionally, use the bar graphs to assess the number WLANs utilized by supported radio bands.

  Periodically select **Refresh** (at the bottom of the screen) to update the radio information.
- The WLAN Utilization table displays the top 5 WLANs utilized by this access point in respect to client support. The first table lists the total number of WLANs managed by this system. The second table lists the top five (5) WLANs in terms of the usage percentage along with their name and network identifying SSID. The utilization index measures how efficiently the RF medium is utilized. It is defined as a percentage of the current throughput relative to the maximum throughput possible.

  The quality is measured as:
  - 0-20 – Very low utilization
  - 20-40 – Low utilization
  - 40-60 – Moderate utilization
  - 60 and above – High utilization

  Periodically select **Refresh** (at the bottom of the screen) to update WLAN utilization information.
- The Wireless Clients table displays information about the wireless clients managed by the selected access point. Information is presented in two (2) tables and a graph. The first table lists the total number of clients managed by the listed access point. The second lists the top five (5) radios in terms of the number of connected clients. The graph just below the table lists the number of clients by radio type.

## Network View

The Network View screen displays device topology association between a selected access point, its RF Domain and its connected clients.

Access points and clients can be selected and viewed using various color schemes in respect to neighboring access points, connected devices and performance criteria. Display options can be utilized to review device performance and utilization, as well as the RF band, channel and vendor. For more information, see Network View Display Options on page 56.

To review a device's network topology, select **Dashboard → Network View**.

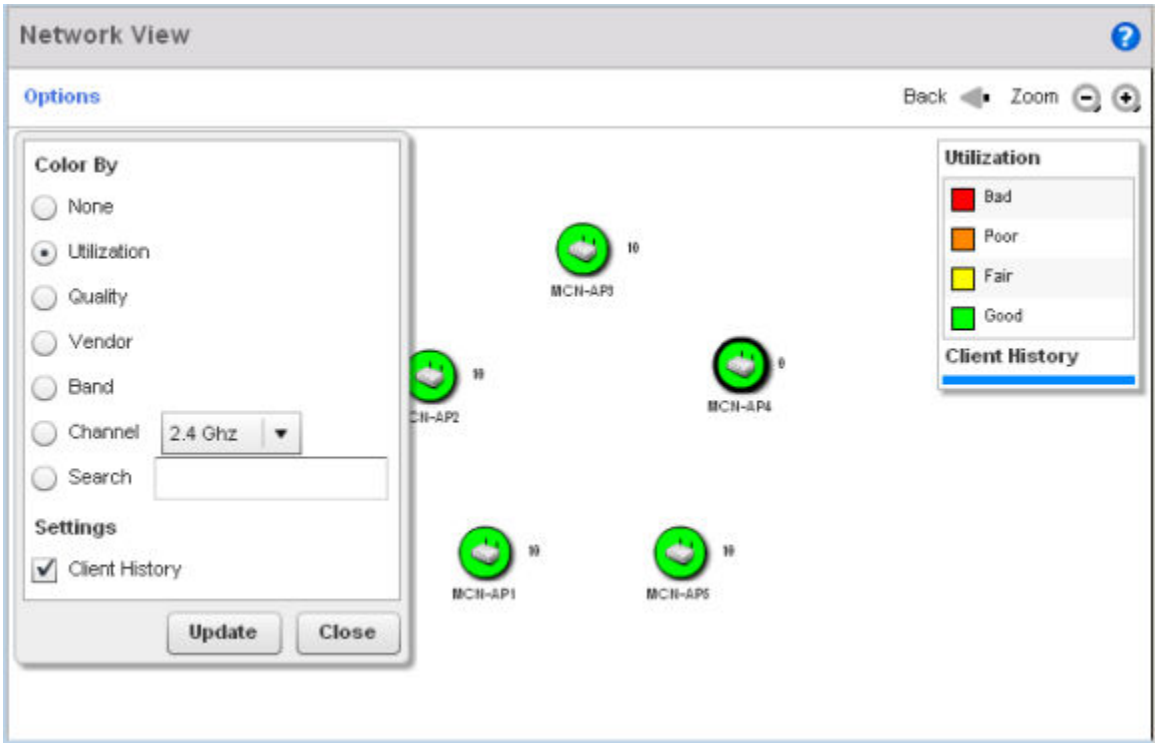



**Figure 10: Network View Topology**

The left side of the Network View screen contains an expandable System browser where access points can be selected and expanded to display connected clients. Navigate the System browser to review device connections within the access point managed network. Many of these peer access points are available for connection to access points in Virtual Controller AP mode.

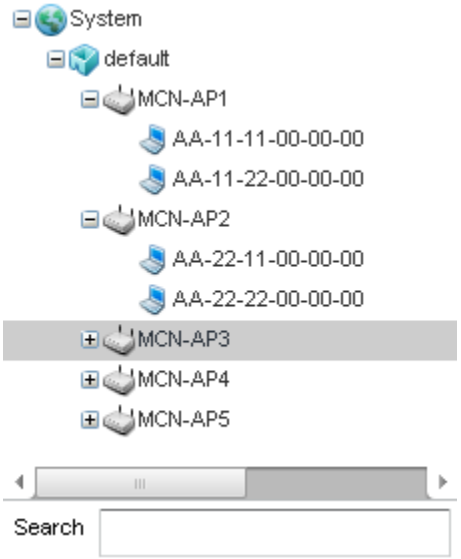



**Figure 11: Network View - System Browser**

*Network View Display Options*

To use the Network View options:

1 Select the blue **Options** link right under the Network View banner to display a menu for different device interaction display options.

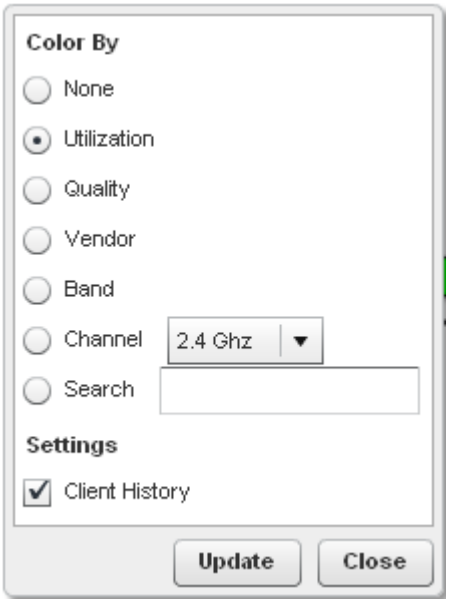



**Figure 12: Network View - Display Options**

The following display filter options are available:

| | |
|---|---|
| None | Select this option to keep the Network View display as it currently appears, without any additional color or device interaction adjustments. |
| Utilization | Select this option to filter based on the percentage of current throughput relative to maximum throughput. Utilization results include: Red (Bad Utilization), Orange (Poor Utilization), Yellow (Fair Utilization) and Green (Good Utilization). |
| Quality | Select this option to filter based on the overall RF health. RF health is a ratio of connection rate, retry rates, and error rates. Quality results include: Red (Bad Quality), Orange (Poor Quality), Yellow (Fair Quality) and Green (Good Quality). |
| Vendor | Displays the device manufacturer. |
| Band | Select this option to filter based on the 2.4 or 5.0 GHz radio band of connected clients. Results include: Yellow (2.4 GHz radio band) and Blue (5.0 GHz radio band). Selecting band is a good way to determine whether 2.4 and 5.0 GHz radios are optimally deployed in respect to the access point client loads on both bands. |
| Channel | Use this drop-down menu to filter whether device connections should be displayed in either the 2.4 or 5.0 GHz band. |
| Search | Enter search criteria in the provided text field and select the Update button to isolate located variables in blue within the Network View display. |

2 Select **Update** to update the display with changes made to the filter options.

3 Select **Close** to close the options field and remove it from the Network View.

*Device Specific Information*

A device-specific information screen is available for individual devices selected from within the Network View.

This screen displays the name assigned to the access point, its model, factory encoded MAC address, number of radios within the device, number of connected clients, as well as the highest and lowest reported quality, utilization and SNR *(Signal to Noise Ratio)*. This information cannot be modified by the administrator.

To view device-specific information:

1 Go to **Dashboard → Network View**.
2 Expand the **System** node to display associated RF Domains.
3 Expand the desired RF Domain node to display associated devices.
4 Double-click on the desired access point. The device-specific information screen displays.

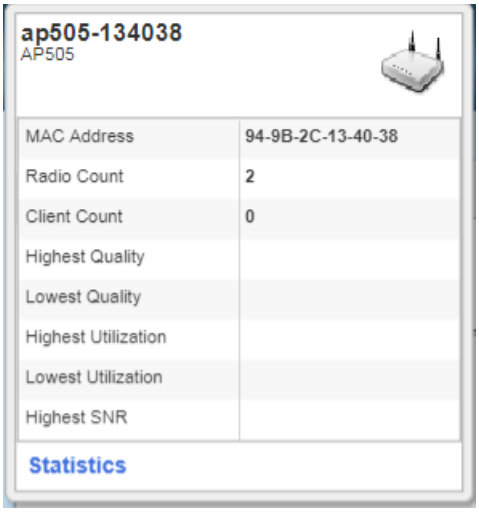



**Figure 13: Network View - Device Specific Information**

Optionally select the **Statistics** link at the bottom of the display to open a screen where access point device data can be reviewed on a much more granular level. For more information, see Access Point Health on page 50.

# 6 Device Configuration



Access points can either be assigned unique configurations to support a particular deployment objective or have an existing RF Domain or profile configuration modified (overridden) to support a requirement that deviates its configuration from the configuration shared by its peer access points.

An RF Domain allows an administrator to assign comparable configuration data to multiple access points deployed in a common coverage area (floor, building or site). In such instances, there are many configuration attributes these devices share, as their general client support roles are quite similar. However, access point configurations may need periodic refinement and overrides from their original RF Domain administered design. For more information, see RF Domain on page 58 .

Profiles enable administrators to assign a common set of configuration parameters and policies to access points of the same model. Profiles can be used to assign shared network, wireless and security parameters to access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. To define a specific access point model profile configuration, refer to System Profile Configuration on page 72.

However, device profile configurations may need periodic refinement from their original administered design. Consequently, a device profile could be applied an override from a configuration shared amongst numerous peer devices deployed within a particular site.

## RF Domain

An access point's configuration consists of numerous elements including an RF Domain, WLAN and device specific settings. RF Domains are used to assign regulatory, location and relevant policies to access points of the same model. For example, an AP 6532 RF Domain can only be applied to another AP 6532 model access point.

An RF Domain allows an administrator to assign configuration data to multiple access points deployed in a common coverage area (floor, building or site). In such instances, there are many configuration attributes these access points share, as their general client support roles are quite similar.

However, an access point's RF Domain configuration may need periodic refinement from its original RF Domain designation. Unlike a RFS series wireless controller, an access point supports just a single RF domain. Thus, administrators should be aware that overriding an access point's RF Domain configuration results in a separate configuration that must be managed in addition to the RF Domain

configuration. Thus, a configuration should only be overridden when needed. For more information, see RF Domain Overrides in the AP Device Context.

The access point's RF Domain can have a WIPS sensor configuration applied. For more information on defining a WIPS sensor configuration for use with the access point's RF Domain, see RF Domain Sensor Configuration on page 61 .

Note

The WiNG 7.1 OS enforces interoperability with access points running the WiNG 5.9.X OS. WiNG 7.1 wireless controllers and service platforms are capable of provisioning and managing both WiNG 5.9.X and WiNG 7.1 APs.

If you have a mixed deployment, with access points running both WiNG 7.1 and WiNG 5.9.X firmware, we recommend that you place these APs in separate RF Domains.

To review the configurations of existing RF Domains:

1 Go to **Configuration → Devices**.

The RF Domain screen displays.

2 Use the following (read-only) information to determine whether the RF Domain policy needs to be edited.

| | |
|---|---|
| RF Domain | Lists each policy's name, as assigned when it was created. The RF Domain name cannot be changed as part of the edit process. Only one RF Domain can be assigned to a controller or access point at one time. |
| Location | Displays the physical location assigned to the RF Domain. This name could be as specific as the floor of a building, or as generic as an entire site. The location defines the physical area where a common set of devices are deployed using the policy's RF Domain configuration. |
| Contact | Lists the contact (administrator) assigned to respond to events created by, or impacting, each listed RF Domain. |
| Time Zone | Displays the geographic time zone set for each RF Domain policy. RF Domains can contain unique country codes and time zone information for controllers and access points deployed across different states or countries, thus making them ideal for managing device configurations across different geographical deployments. |
| Country Code | Display the two-digit country code set for the policy. The country code must be set accurately to avoid illegal operation, as device radios transmit in specific channels unique to their country of operation. |

## RF Domain Basic Configuration

An administrator can only edit, rename or replace an access point's RF Domain assignment.

To edit an RF Domain's configuration:

1 On the RF Domain screen, select the RF Domain by double-clicking on it.

The RF Domain Basic Configurationtab displays by default with the access point's RF Domain activated.

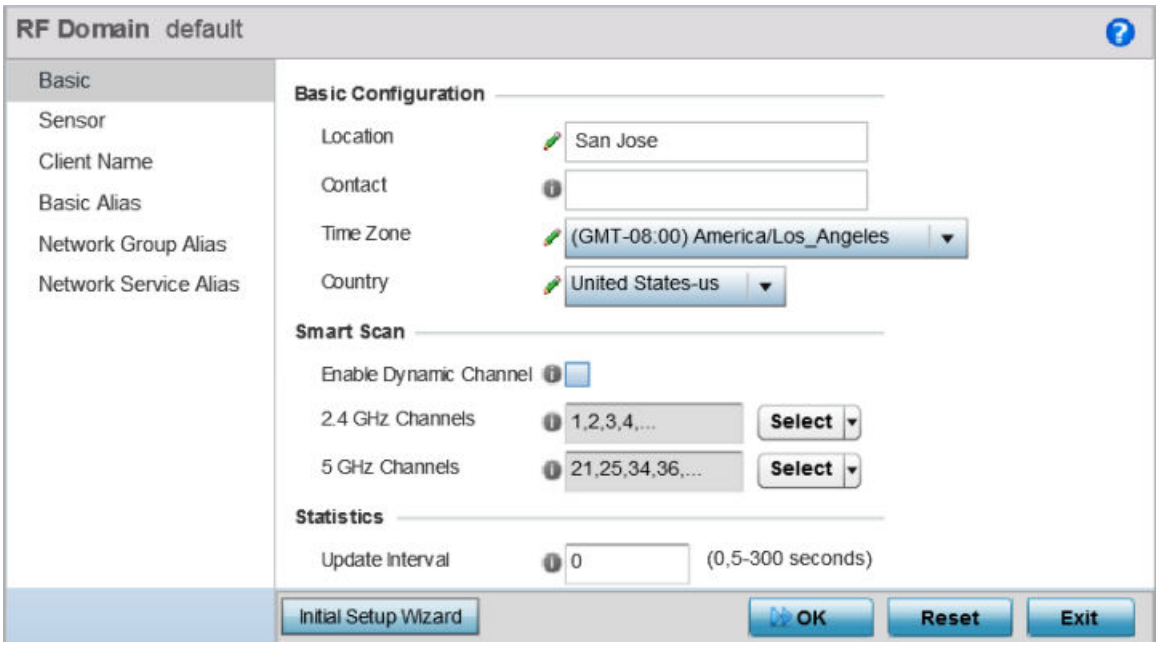



**Figure 14: RF Domain - Basic Configuration Tab**

2 Define the following Basic Configuration values:

| | |
|---|---|
| Location | Assign the physical location of the RF Domain. This name could be as specific as the floor of a building, or as generic as an entire site. The location defines the physical area where a common set of access point configurations are deployed and managed by the RF Domain policy. |
| Contact | Provide the name of the contact E-mail (or administrator) assigned to respond to events created by or impacting the RF Domain. |
| Time Zone | Set the geographic time zone for the RF Domain. The RF Domain can contain unique country codes and time zone information to access points deployed across different states or countries, thus making them ideal for managing device configurations across different geographical deployments. |
| Country | Define the two-digit country code set for the RF Domain. The country code must be set accurately to avoid the policy's illegal operation, as device radios transmit in specific channels unique to the country of operation. |

3 Refer to the Smart Scan field to define the channels for smart scan.

| | |
|---|---|
| Enable Dynamic Channel | Select this option to enable channel scan. |
| 2.4 GHz Channels | Use the **Select** drop-down menu to select channels to scan in the 2.4 GHz band. Selected channels are highlighted with a grey-colored background. Unselected channels are highlighted with a white-colored background. Multiple channels can be selected at the same time. |
| 5.0 GHz Channels | Use the **Select** drop-down menu to select channels to scan in the 5.0 GHz band. Selected channels are highlighted with a grey-colored background. Unselected channels are highlighted with a white-colored background. Multiple channels can be selected at the same time. |

4 Refer to the Statistics field to define how RF Domain statistics are updated.

| | |
|---|---|
| Update Interval | Set a statistics update interval of 0 or 5-3600 seconds for updates retrieved from the access point. The default value is 0. |

5 Use the Initial Setup Wizard to configure the device.

6 Select **OK** to save the changes to the Basic Configuration.

Click **Reset** to revert to the last saved configuration.

## RF Domain Sensor Configuration

WIPS *(Wireless Intrusion Protection System)* protects wireless client and access point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgment of a threat.

In addition to dedicated AirDefense sensors, an access point radio can function as a sensor and upload information to a dedicated WIPS server (external to the access point). Unique WIPS server configurations can be used to ensure a WIPS server configuration is available to support the unique data protection needs of a RF Domain.

WIPS is not supported on a WLAN basis, rather, sensor functionality is supported on the access point radio(s) available to each managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all legal channels within the 2.4 and 5.0 GHz band. Sensor support requires an AirDefense WIPS Server on the network. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server.

In addition to WIPS support, sensor functionality has been added for Extreme Networks' ExtremeLocation system. locationing system. The ExtremeLocation system for Wi-Fi locationing includes WiNG controllers and access points functioning as sensors. Within the ExtremeLocation architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated ExtremeLocation Server resource, as opposed to an ADSP server. The ExtremeLocation Server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices.

To define a WIPS server configuration used with the access point's RF Domain:

1 Go to **Configuration → Devices**.

2 Select an **RF Domain** from those listed on left-hand side of the UI.

The RF Domain configuration menu displays in the left-hand UI.

3 Select **Sensor**.

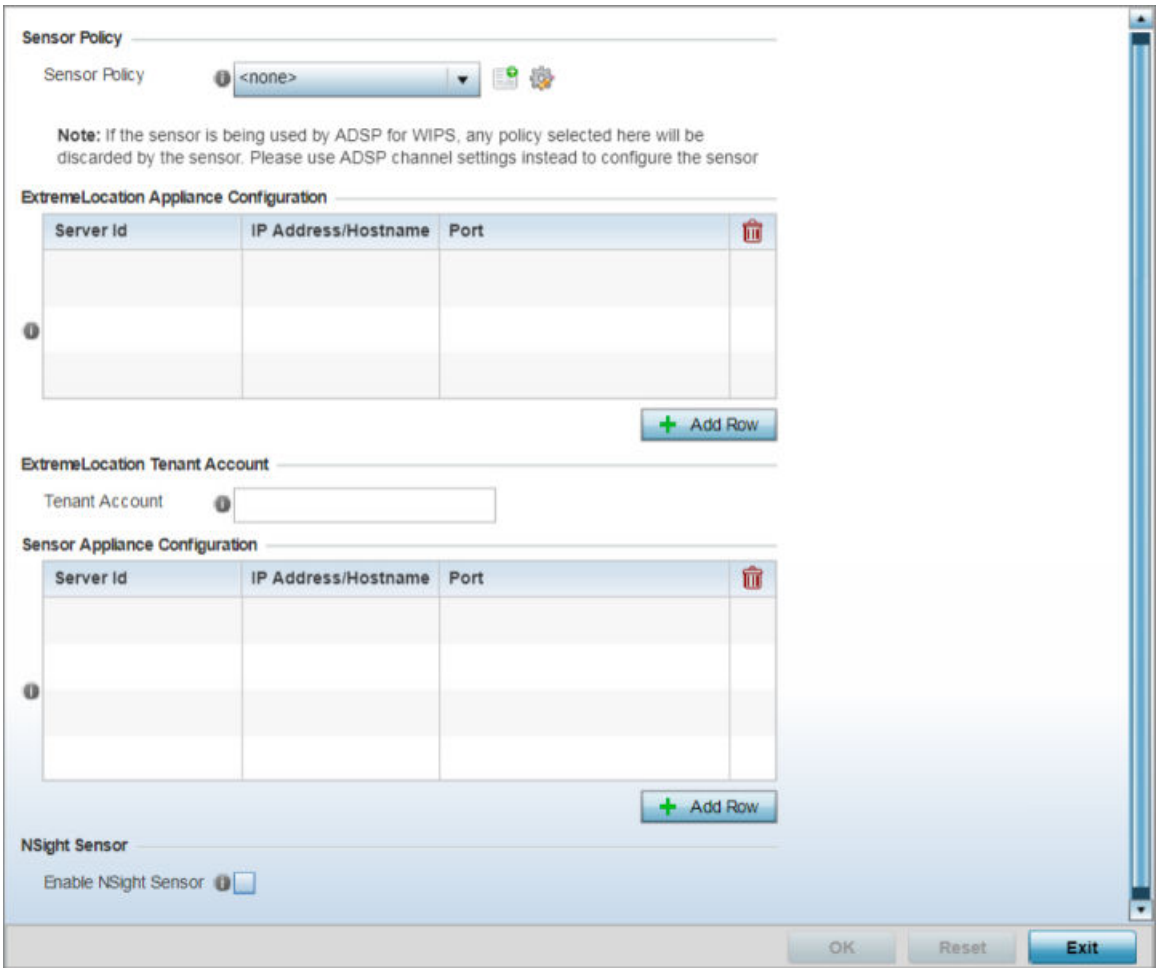



**Figure 15: RF Domain - Sensor Configuration screen**

4 Use the **Sensor Policy** drop-down menu to select a sensor policy for sending RSSI information to a dedicated system for device locationing calculations. Different policies can be created with either a default set of scanned channels or with custom channels, widths and weighted scan priorities. Specific channels can also be isolated and locked for specific channel scans.

Note

If a dedicated sensor is utilized with ADSP for rogue detection, any sensor policy selected from the **Sensor Policy** drop-down menu is discarded and not utilized by the sensor. To avoid this situation, use ADSP channel settings exclusively to configure the sensor and not the WiNG interface.

5 Select the **Create** icon to create a new sensor policy or select the **Edit** icon to update the configuration of an existing policy. The Sensor Policy addition screen displays with the *Scan Mode* set to *Default-Scan*. The user configurable parameters available within the screen differ depending on the Scan Mode option selected. For more information, see Sensor Policy on page 671.

6 In the ExtremeLocation Appliance Configuration field, select the **+ Add Row** button to populate the ExtremeLocation server details.

Within the ExtremeLocation Appliance architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated ExtremeLocation server resource, as opposed to an ADSP server.

| | |
|---|---|
| Server Id | Use the spinner control to assign a numerical ID for the ExtremeLocation server resource.<br><br>Note: As of now only one server is supported. |
| IP Address/Hostname | Provide the hostname of the ExtremeLocation server resource for receiving RSSI scan data from the AP. Hostname cannot exceed 64 characters or contain an underscore.<br><br>Note: Enter the ExtremeLocation server's hostname and not the IP address, as the IP address is likely to change periodically in order to balance load across multiple Location server instances. |
| Port | Use the spinner control to specify the port of the ExtremeLocation sensor server resource receiving RSSI scan data from a dedicated sensor. The default port is 443. |

7 Enter the `ExtremeLocation Tenant's account number` in the **Tenant Account** field.

Use this field to configure your ExtremeLocation Tenant account number. Every Tenant, subscribing for the ExtremeLocation service, is communicated (via, email) an account number that uniquely identifies the Tenant. When configured in the RF Domain context, reports pushed to the ExtremeLocation server by RF Domain APs contain this account number. Including the Tenant account number reinforces the Tenant's identity.

8 Select the **Enable NSight Sensor** checkbox to enable the NSight module

9 Select **OK** to save the changes to the Sensor configuration.

Click **Reset** to revert to the last saved configuration.

## RF Client Name Configuration

The RF Domain Client Name Configuration screen displays clients connected to RF Domain member access points adopted by networked controllers or service platforms. Use the screen to associate administrator assigned client names to specific connected client MAC addresses for improved client management.

To define a client name configuration used with RF Domain member devices:

1 Go to **Configuration → Devices**.

2 Select an **RF Domain** from those listed on left-hand side of the UI.

The RF Domain configuration menu displays in the left-hand UI.

3 Select Client Name.

The Client Name Configuration screen displays.

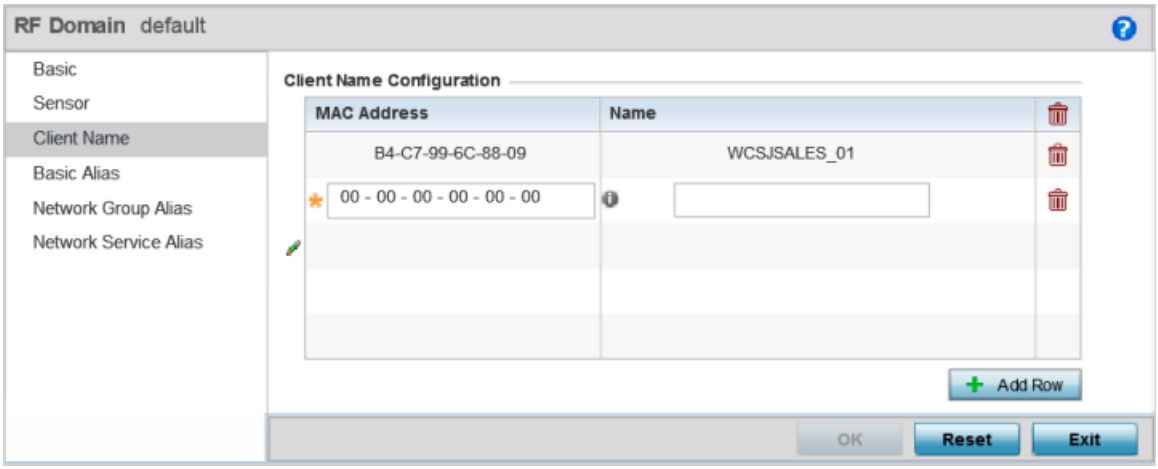



**Figure 16: RF Domain - Client Name Configuration Screen**

4 Either select the **+ Add Row** button to create a new client configuration or highlight an existing configuration and select the **Delete** icon to remove it.

5 Enter the client's factory coded `MAC Address`.

6 Assign a `Name` to the RF Domain member access point's connected client to assist in its easy recognition.

7 Click **OK** to save the changes to the configuration.

Click **Reset** to revert to the last saved configuration.

## RF Domain Alias Configuration

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the alias is defined. Alias are defined with the following scopes:

- Global aliases are defined from the **Configuration → Network → Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- Profiles aliases are defined from **Configuration → Devices → System Profile → Network → Alias** screen. These aliases are available for use to a specific group of wireless controllers or access points. Alias values defined in this profile override alias values defined within global aliases.
- RF Domain aliases are defined from **Configuration → Devices → RF Domain → Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- Device aliases are defined from **Configuration → Devices → Device Overrides → Network → Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an Network Alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias works with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Alias can be classified as:

- Basic Alias on page 65
- Network Group Alias on page 68
- Network Service Alias on page 70

### *Basic Alias*

A basic alias is a set of configurations that consist of VLAN, Host, Network and Address Range alias configurations. VLAN configuration is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

A basic alias configuration can contain multiple instances for each of the five (5) alias types.

To edit or delete a basic alias configuration:

1 Go to **Configuration → Devices**.

2 Select an **RF Domain** from the options on left-hand side of the UI, and then go to the Basic Alias tab.

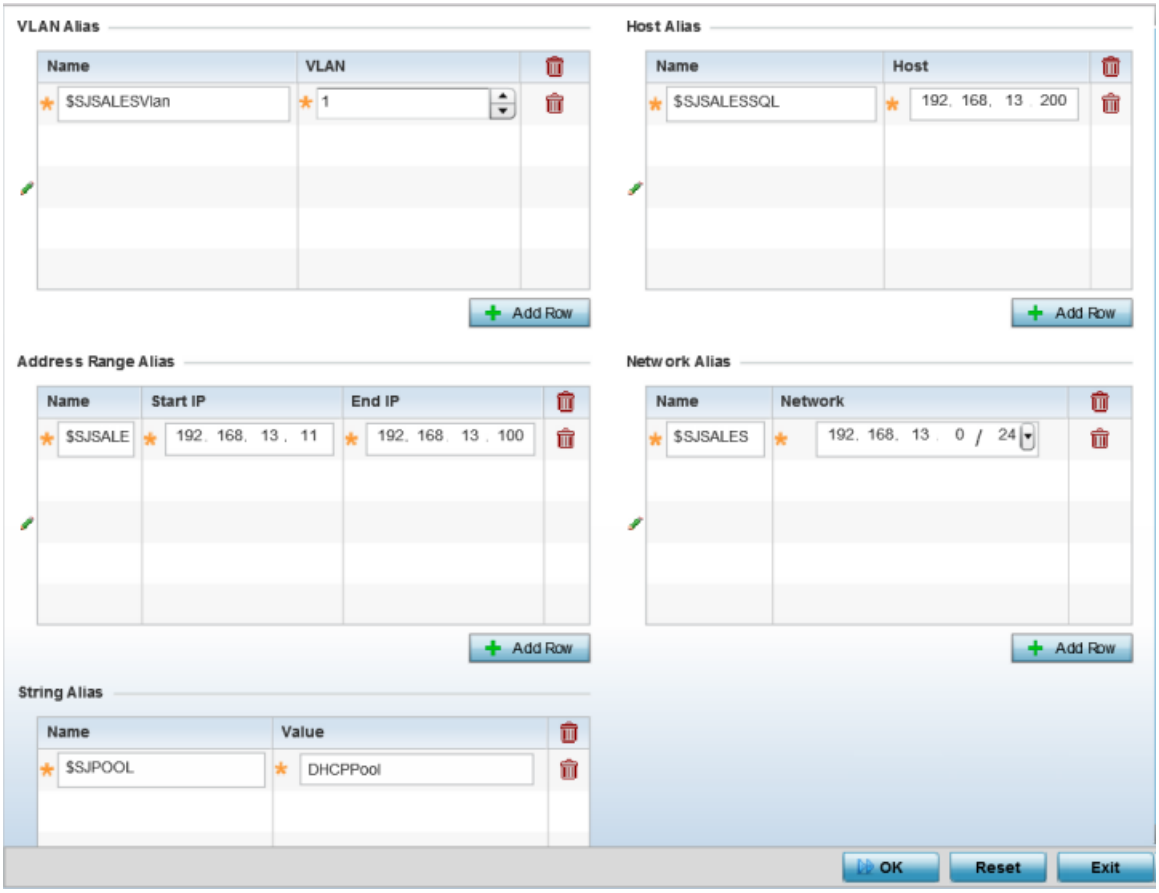



**Figure 17: RF Domain - Basic Alias screen**

3 Select **+ Add Row** to define VLAN Alias settings.

4 Use the VLAN Alias field to create unique aliases for VLANs that can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

| | |
|---|---|
| Name | If adding a new VLAN Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| VLAN | Use the spinner control to set a numeric VLAN from 1 - 4094. |

A VLAN alias can be used to replace VLANs in the following locations:

- Bridge VLAN
- IP Firewall Rules
- L2TPv3
- Switchport
- Wireless LANs

5 Select **+ Add Row** to define Address Range Alias settings.

6 Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

| | |
|---|---|
| Name | If adding a new Address Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Start IP | Set a starting IP address used with a range of addresses utilized with the address range alias. |
| End IP | Set a ending IP address used with a range of addresses utilized with the address range alias. |

An address range alias can be used to replace an IP address range in IP firewall rules.

7 Select **+ Add Row** to define **Host Alias** settings:

8 Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new Host Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Host | Set the IP address of the host machine. |

A host alias can be used to replace hostnames in the following locations:

- IP Firewall Rules
- DHCP

9 Select **+ Add Row** to define **Network Alias** settings:

10 Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new Network Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Network | Provide a network address in the form of host/mask. |

A network alias can be used to replace network declarations in the following locations:

- IP Firewall Rules
- DHCP

11 Select **+ Add Row** to define **String Alias** settings.

12 Use the **String Alias** field to create aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location

to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

| | |
|---|---|
| Name | If adding a new String Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Value | Provide a string value to use in the alias. |

A string alias can be used to replace a domain name string in DHCP.

13 Select **OK** when completed to update the basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

*Network Group Alias*

A network group alias is a set of configurations that consist of host and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20. Host configuration is in the form of single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for host, network, and IP address range. A maximum of eight (8) host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

A network group alias is used in IP firewall rules to substitute hosts, subnets and IP address ranges:

To edit or delete a network alias configuration:

1 Go to **Configuration** → **Devices**.

2 Select an **RF Domain** from the options on left-hand side of the UI, and then go to the Network Group Alias tab.

The Network Group Alias screen displays.

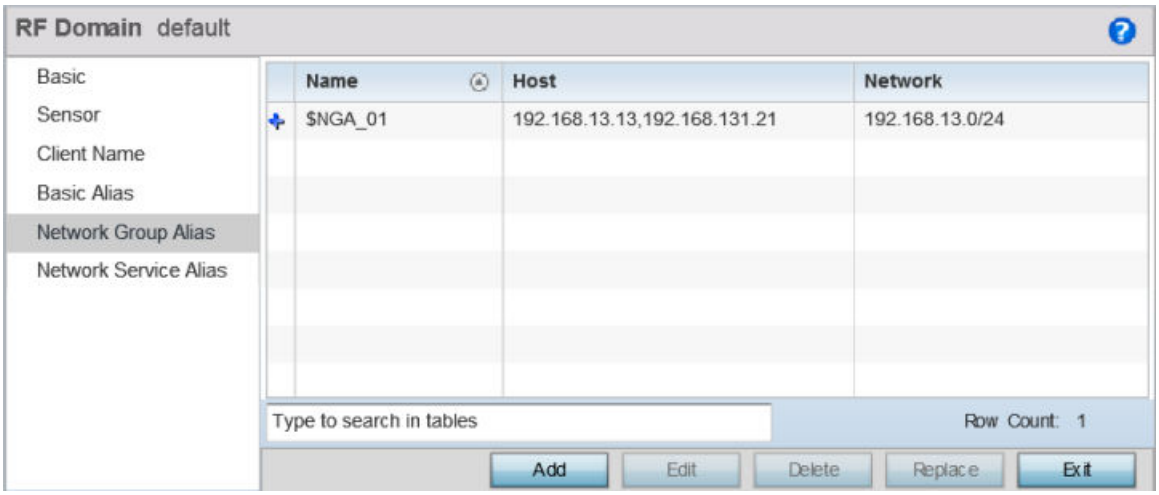



**Figure 18: RF Domain - Network Group Alias screen**

3 Review the following information to determine if an existing alias configuration needs modification or deletion. Or, if a new alias needs to be created.

| | |
|---|---|
| Name | Displays the administrator assigned name of the network group alias. |
| Host | Displays all host aliases configured in this network group alias. Displays a blank column if no host alias is defined. |
| Network | Displays all network aliases configured in this network group alias. Displays a blank column if no network alias is defined. |

### Adding/Editing Network Group Alias

You can add a new network group alias, or edit an existing alias.

1 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new network group alias. Select **Copy** to copy an existing policy or **Rename** to rename an existing policy.

2 If adding a new network group alias, provide it a name of up to 32 characters.

Note

The network group alias name always starts with a dollar sign ($).

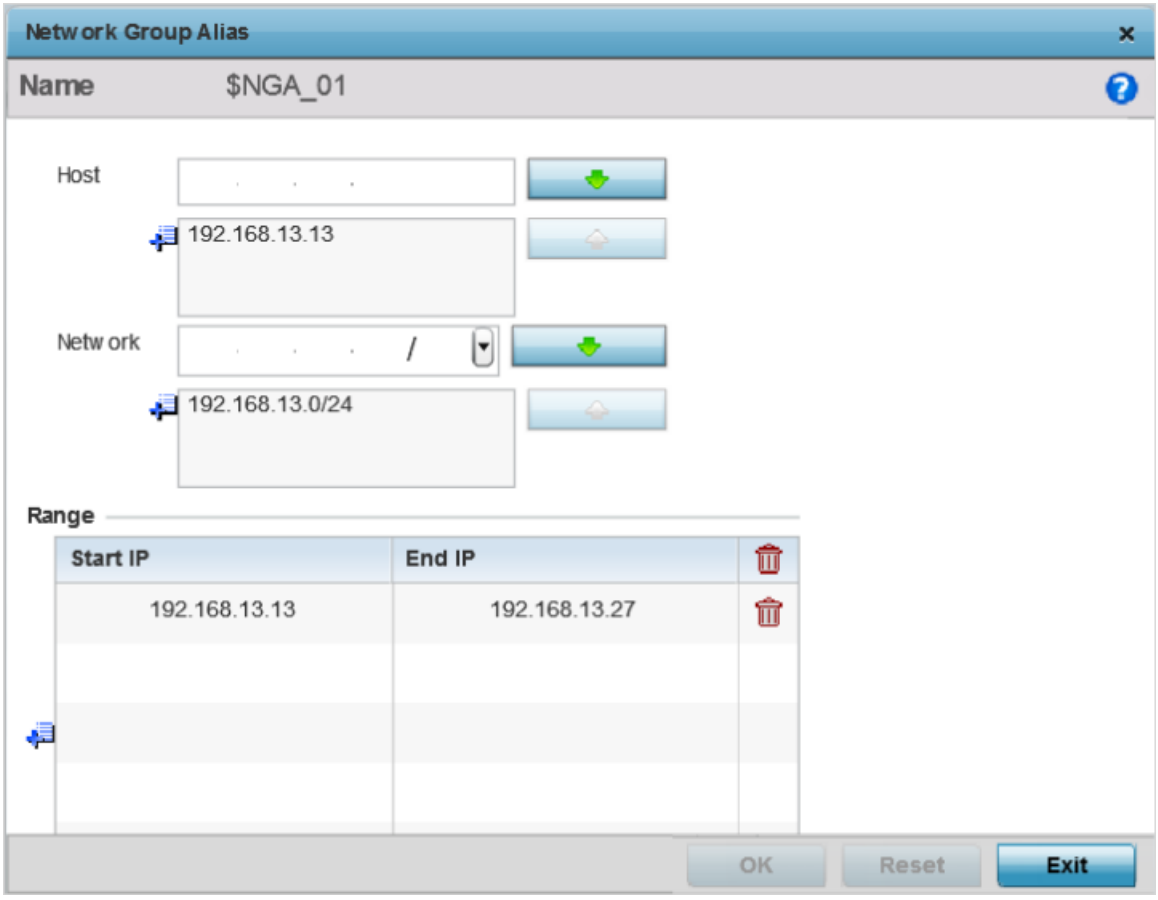



**Figure 19: RF Domain - Network Group Alias Add screen**

3 Define the following network group alias parameters:

| | |
|---|---|
| Host | Specify the host IP address. You can add up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table. |
| Network | Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table. |

4 Within the Range table, use the **+ Add Row** button to specify the Start IP address and End IP address for the alias range or double-click on an existing alias range entry to edit it.

5 Select **OK** when completed to update the network group alias rules. Select **Reset** to revert the screen back to its last saved configuration.

*Network Service Alias*

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

Network service aliases can be used in the following location to substitute protocols and ports:

- IP Firewall Rules

The Network Service Alias main screen displays existing network service aliases,

To edit or delete a service alias configuration:

1 Go to **Configuration → Devices**.

2 Select an **RF Domain** from the options on left-hand side of the UI, and then go to the Network Service Alias tab.

The screen displays network service aliases existing within the managed system.

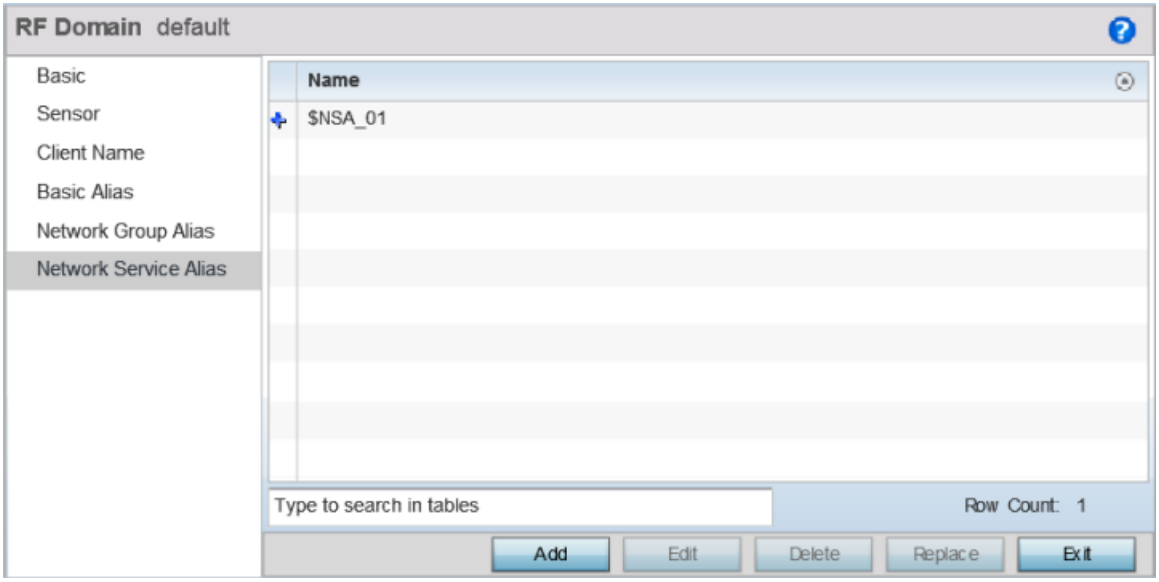



**Figure 20: RF Domain - Network Service Alias screen**

### Adding/Editing Network Service Alias

You can add a new network service alias, or edit an exisitng network service alias.

1 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new Network Service Alias.

2 If adding a new network service alias, provide it a name of up to 32 characters.

Note

The network service alias name always starts with a dollar sign ($).

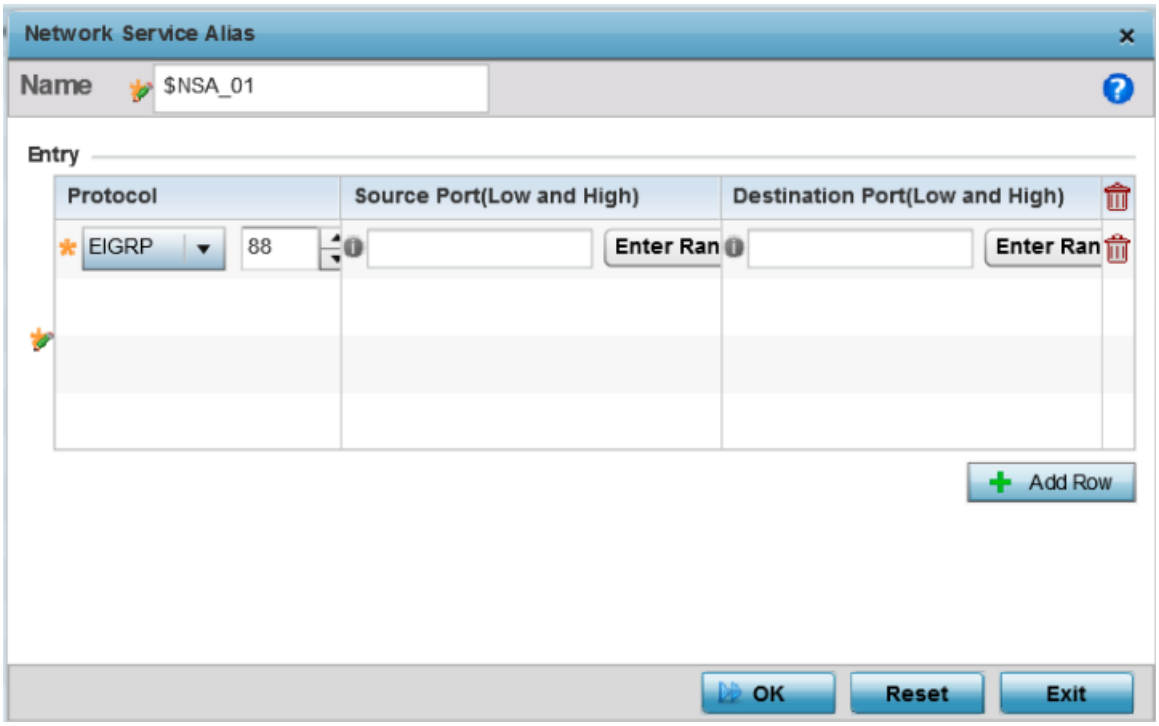



**Figure 21: RF Domain - Network Service Alias Add screen**

3 Within the Range field, use the **+ Add Row** button to specify the Start IP address and End IP address for the service alias range or double-click on an existing service alias range entry to edit it.

| | |
|---|---|
| Protocol | Specify the protocol for which the alias has to be created. Use the drop-down menu to select the protocol (eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp and udp). Select other if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected. |
| Source Port (Low and High) | Use this field only if the protocol is tcp or udp. Specify the source ports for this protocol entry. A range of ports can be specified. Select the Enter Range button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified. |
| Destination Port (Low and High) | Use this field only if the protocol is tcp or udp. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the Enter Range button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified. |

4 Select **OK** when completed to update the network service alias rules.

Select **Reset** to revert the screen back to its last saved configuration.

## System Profile Configuration

An access point profile enables an administrator to assign a common set of configuration parameters and policies to access points of the same model. Profiles can be used to assign common or unique network, wireless and security parameters to across a large, multi-segment site. The configuration parameters within a profile are based on the hardware model the profile was created to support. All WiNG OS supported access point models supported a single profile that is either shared amongst multiple access point or not. The central benefit of a profile is the ability to update access points collectively without having to modify individual configurations.

A profile allows access point administration across large wireless network segments. However, an administrator cannot manage more than one model's profile and its set configuration policies at any one time. Therefore, an administrator should manage multiple access points directly from the Virtual Controller AP. As individual access point updates are made, the access point no longer shares the profile based configuration it previously deployed. Changes made to the profile are automatically inherited by all member access points, but not those who have had their configuration overridden from their previous profile designation. These devices require careful administration, as they no longer can be tracked and as profile members. Their customized configurations overwrite their profile assignments until the profile can be re-applied to the access point.

Each access point model is automatically assigned a default profile. The default profile is available within the access point's configuration file. Default profiles are ideal for single-site deployments where several access points may need to share a common configuration.

Note

Default profiles are used as pointers for an access point's configuration, not just templates from which the configuration is copied. Therefore, if a change is made in one of the parameters in a profile, the change is reflected across all access points using that profile.

For more information, refer to the following:


- System Profile Configuration - General Screen on page 73
- Profile Radio Power on page 74
- Profile Adoption (Auto Provisioning) Configuration on page 76
- Profile Wired 802.1X Configuration on page 78
- Profile Interface Configuration on page 79
- Profile Network Configuration on page 145
- Profile Security Configuration on page 216
- Virtual Router Redundancy Protocol on page 252
- List of Critical Resources on page 256
- Profile Services Configuration on page 260
- Management Settings on page 264
- Meshpoint Configuration on page 269
- Environmental Sensor Configuration on page 279
- Advanced Profile Configuration on page 280

## System Profile Configuration - General Screen

An access point profile requires unique clock synchronization settings as part of its general configuration.

The NTP *(Network Time Protocol)* is a client-server implementation that manages time and/or network clock synchronization within the network. Controllers, service platforms, and access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, an access point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

To define a profile's general configuration:

1 Select **Configuration → Devices → System Profile** from the Web UI.

A list of device profiles is displayed in the right-hand UI. This list contains default and user-defined profiles.

2 Select a device profile from the list.

**General** configuration options display by default, with the profile activated for use with this access point model.

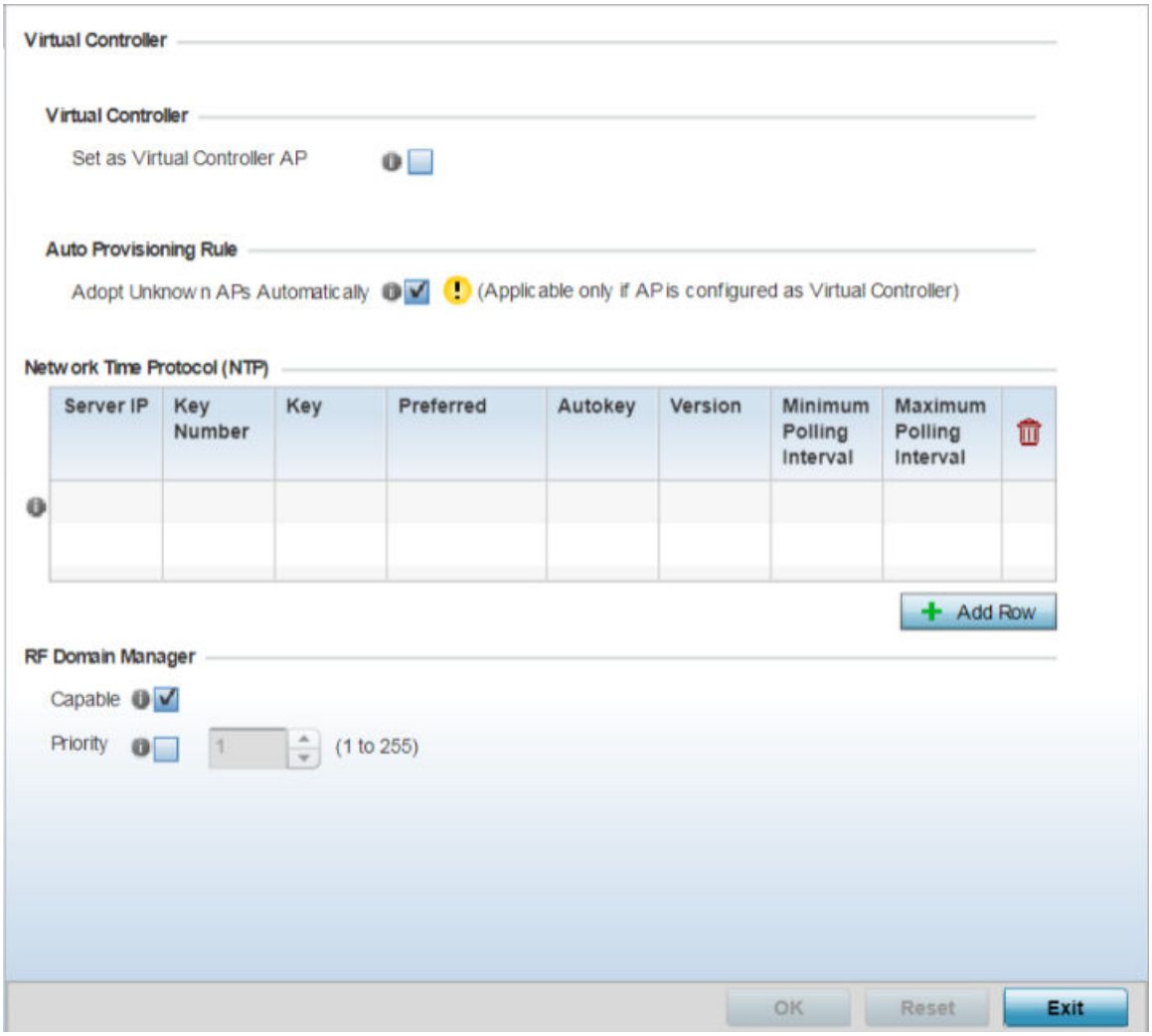



**Figure 22: General Profile Screen**

3 Select the **Set as Virtual Controller AP** checkbox, to configure this AP as VC.

Note
WiNG 7.1 does not support VC configuration on AP505 and AP510 model access points.

4 If you set the AP is a VC, select the **Adopt Unknown APs Automatically** checkbox.

Note
WiNG 7.1 does not support VC configuration on AP505 and AP510 model access points.

5 Select **+ Add Row** below the Network Time Protocol (NTP) table to define the configurations of NTP server resources used to obtain system time. Up to three NTP servers can be configured. Set the following parameters to define the NTP configuration:

| | |
|---|---|
| Server IP | Set the IP address of each server added as a potential NTP resource. |
| Key Number | Select the number of the associated authentication peer key for the NTP resource. |
| Key | Enter a 64 character maximum key used when the autokey setting is set to false (disabled). Select the Show option to expose the actual character string comprising the key. |
| Preferred | Select this option to designate this NTP resource as a preferred NTP resource. This setting is disabled by default. |
| AutoKey | Select the check box to enable an autokey configuration for the NTP resource. The default setting is disabled. |
| Version | Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0. |
| Minimum Polling Interval | Use the drop-down menu to select the minimum polling interval. Once set, the NTP resource is polled no sooner then the defined interval. Options include 64, 128, 256, 512 or 1024 seconds. The default setting is 64 seconds. |
| Maximum Polling Interval | Use the drop-down menu to select the maximum polling interval. Once set, the NTP resource is polled no later then the defined interval. Options include 64, 128, 256, 512 or 1024 seconds. The default setting is 1024 seconds. |

6 Use the RF Domain Manager field to configure how this access point behaves in standalone mode. Set the following parameters:

| | |
|---|---|
| Capable | Select to enable this access point to act as a RF Domain Manager in a particular RF Domain. |
| Priority | Select to prioritize this access point in becoming a RF Domain Manager in its; particular RF Domain. The higher the value, the more likely the device becomes the RF Domain Manager for the domain. |

7 Select **OK** to save the changes made to the general profile configuration.

Select **Reset**to revert to the last saved configuration.

## Profile Radio Power

Use the Power screen to set one of two power modes (3af or Auto) for the access point profile. When Automatic is selected, the access point safely operates within available power. Once the power

configuration is determined, the access point configures its operating power characteristics based on its model and power configuration.

An access point uses a *complex programmable logic device* (CPLD) to manage power. The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the maximum power budget. When an access point is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the access point. The CPLD also determines the access point hardware SKU (model) and the number of radios.

If the access point's POE resource cannot provide sufficient power to run the access point (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- The access point's transmit and receive algorithms could be negatively impacted
- The access point's transmit power could be reduced due to insufficient power
- The access point's WAN port configuration could be changed (either enabled or disabled)

To define an access point's power configuration:

1 Select **Configuration → Devices → System Profile → Power** from the web UI.

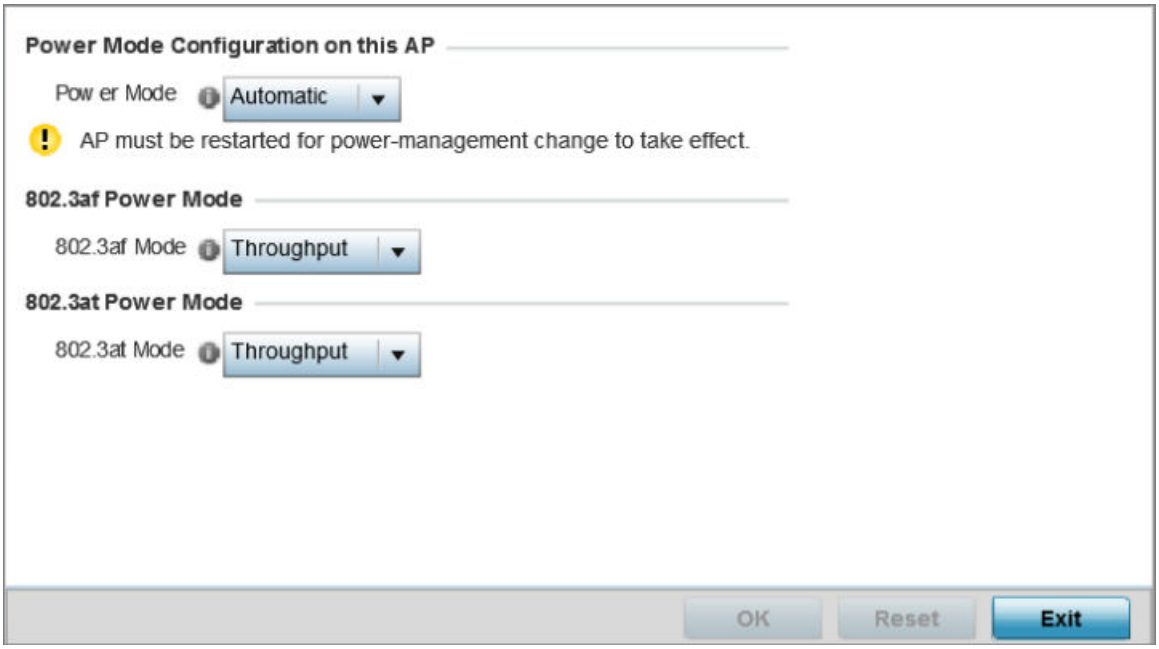



**Figure 23: Device Configuration - System Profile - Power Screen**

2 Use the **Power Mode** drop-down menu to set the Power Mode Configuration on this AP.

Note
Single radio model access points always operate using a full power configuration. The power management configurations described in this section do not apply to single radio access point models.

When an access point is powered on for the first time, it determines the power budget available. Using the **`Automatic`** setting, the access point automatically determines the best power configuration based on the available power budget. Automatic is the default setting.

If **`802.3af`** is selected, the access point assumes 12.95 watts are available. If the mode is changed, the access point requires a reset to implement the change. If 802.3at is selected, the access point assumes 23 - 26 watts are available.

3 Set the access point radio's **802.3af Power Mode** and the radio's **802.3at Power Mode**.

Use the drop-down menu for each power mode to define a mode of either **`Range`** or **`Throughput`**.

Select **Throughput** to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where the transmission range is secondary to broadcast/multicast transmission performance.

Select **Range** when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. Throughput is the default setting for both 802.3af and 802.3at.

4 Select **OK** to save the changes made to the access point power configuration. Select **Reset** to revert to the last saved configuration.

## Profile Adoption (Auto Provisioning) Configuration

Adoption is the process an access point uses to discover an available controller or service platform, pick the most desirable one, establish an association and optionally obtain an image upgrade and configuration. Adoption settings are configurable and supported within a device profile and applied to other access points supported by the profile. Individual attributes of an access point's auto provisioning policy can be overridden as specific parameters require modification.

At adoption, an access point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Modify existing adoption policies or create a new one as needed to meet access point adoption requirements and profile settings.

Note
A device configuration does not need to be present for an auto provisioning policy to take effect. Once adopted, and the device's configuration is defined and applied by the controller, the auto provisioning policy mapping does not have an impact on subsequent adoptions by the same device.

To define the access point profile's adoption configuration:

1 Select **Configuration** → **Devices** → **System Profile** → **Adoption** from the web UI.

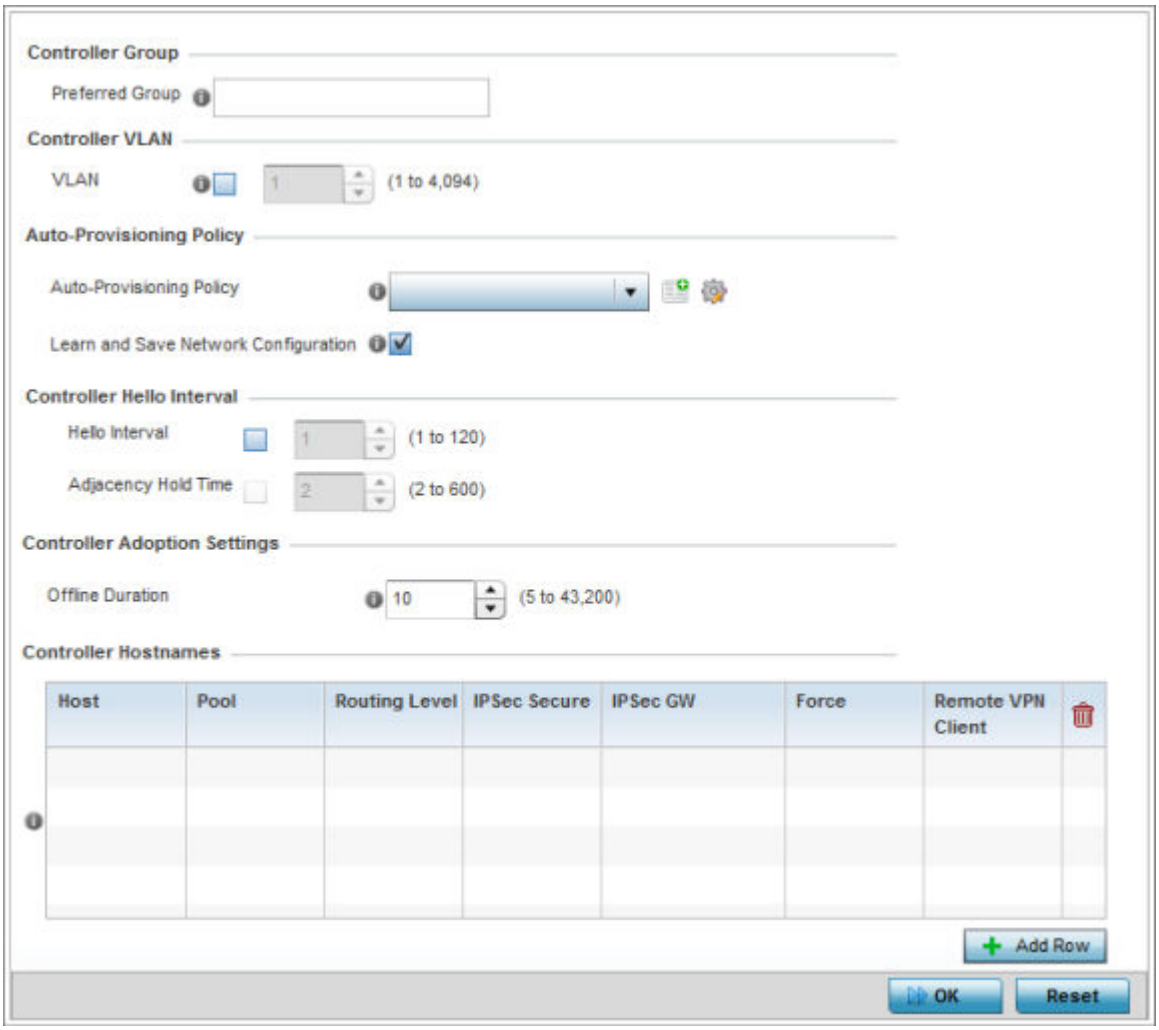



**Figure 24: Device Configuration - System Profile - Adoption Screen**

2 Define the **Preferred Group** used as optimal group of controllers for the access point's adoption. The name of the preferred group cannot exceed 64 characters.

The preferred group is the controller group the access point would prefer to connect upon adoption.

3 Select the **VLAN** option to define a VLAN the access point's associating Virtual Controller AP is reachable on. VLANs 0 and 4,095 are reserved and cannot be used. This setting is disabled by default.

4 Set the following **Auto-Provisioning Policy** settings for access point adoptions:

| | |
|---|---|
| Auto-Provisioning Policy | Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the **Create** icon or modify an existing one by selecting the **Edit** icon. |
| Learn and Save Network Configuration | Select this option to enable allow the controller tor service platform to maintain a local configuration records of devices requesting adoption and provisioning. This feature is enabled by default. |
| Hello Interval | Select this option to define the hello packet exchange interval (from 1 - 120 seconds) between the controller or service platform and an adoption requesting access point. |

5 Define the **Hello Interval** value in seconds.

The Hello interval is the interval between two consecutive hello keep alive messages exchanged between the access point and the adopting wireless controller. These messages serve as a connection validation mechanism to ensure the availability of the adopting wireless controller. Use the spinner to set a value from 1 - 120 seconds.

6 Define the **Adjacency Hold Time** value. This value sets the time after which the preferred controller group is considered down and unavailable to provide services. Use the spinner to set a value from 2 - 600 seconds.

7 Enter **Controller Hostnames** as needed to define resources for adoption. Click **+Add Row** to add controllers. Set the following parameters to define Controller Hostnames:

| | |
|---|---|
| Allow Adoption of Devices | Select either **`access points`** or **`Controllers`** (or both) to refine whether this controller or service platform can adopt just networked access points or peer controller devices as well. |
| Allow Adoption of this Controller | Select this option to enable this controller or service platform to be capable of adoption by other controllers or service platforms. This setting is disabled by default and must be selected to allow peer adoptions. |
| Preferred Group | If Allow Adoption of this Controller is selected, provide the controller group preferred as the adopting entity for this controller or service platform. If utilizing this feature, ensure the appropriate group is provided within the Controller Group field. |
| Hello Interval | Select this option to define the hello packet exchange interval (from 1 - 120 seconds) between the controller or service platform and an adoption requesting access point. |
| Adjacency Hold Time | Select this option to set a hold time interval (from 2 - 600 seconds) for the transmission of hello packets. |

8 Select **+ Add Row** as needed to populate the table with IP addresses or hostnames of adoption resources.

9 Select **OK** to save the changes made to the general profile configuration. Select **Reset** to revert to the last saved configuration.

## Profile Wired 802.1X Configuration

802.1X provides administrators secure, identity based access control as another data protection option to utilize with a device profile.

802.1X is an IEEE standard for media-level (Layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity.

1 Select **Configuration** → **Devices** → **System Profile** → **Wired 802.1x** from the web UI.

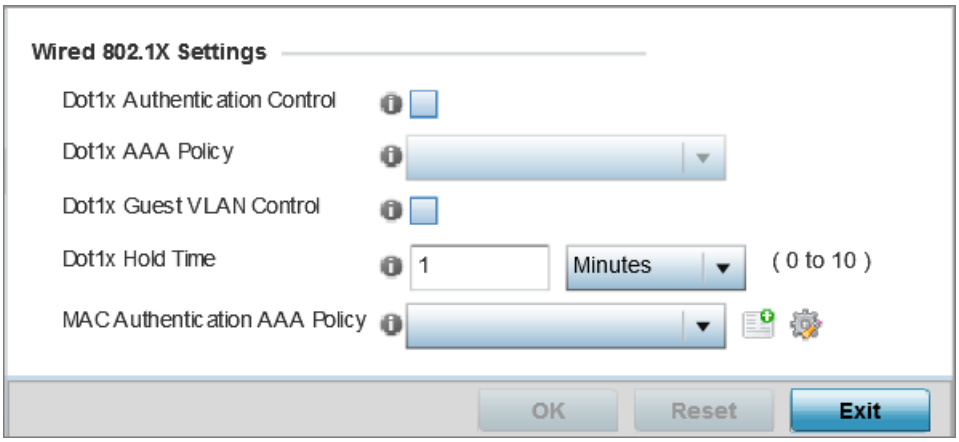



**Figure 25: Device Configuration - System Profile - Wired 802.1X screen**

2 Review the **Wired 802.1x Settings** area to configure the following parameters:

| | |
|---|---|
| Dot1x Authentication Control | Select this option to globally enable 802.1x authentication. 802.1x authentication is disabled by default. |
| Dot1x AAA Policy | Select a AAA policy to associate with wired 802.1x traffic. If a suitable AAA policy does not exist, click the **Create** icon to create a new policy or the **Edit** icon to modify an existing policy. |
| Dot1x Guest VLAN Control | Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default. |
| MAC Authentication AAA Policy | Select a AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the **Create** icon to create a new policy or the **Edit** icon to modify an existing policy. |

3 Click **OK** to save the changes made to the 802.1x configuration.

Click **Reset** to revert to the last saved configuration.

## Profile Interface Configuration

A access point profile can support customizable Ethernet port, virtual interface, port channel, radio and PPPoE configurations unique to each supported access point model.

A profile's interface configuration process consists of the following:

- Ethernet Port Configuration on page 80
- Virtual Interface Configuration on page 91
- Port Channel Configuration on page 107
- Access Point Radio Configuration on page 114
- PPPoE Configuration on page 138
- Bluetooth Configuration on page 141

Additionally, deployment considerations and guidelines for profile interface configurations are available for review prior to defining a configuration that could significantly impact the performance of the network. For more information, see WAN Backhaul Deployment Considerations on page 138.

*Ethernet Port Configuration*

To define a profile's physical Ethernet port configuration:

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Interface** menu and select **Ethernet Ports**.

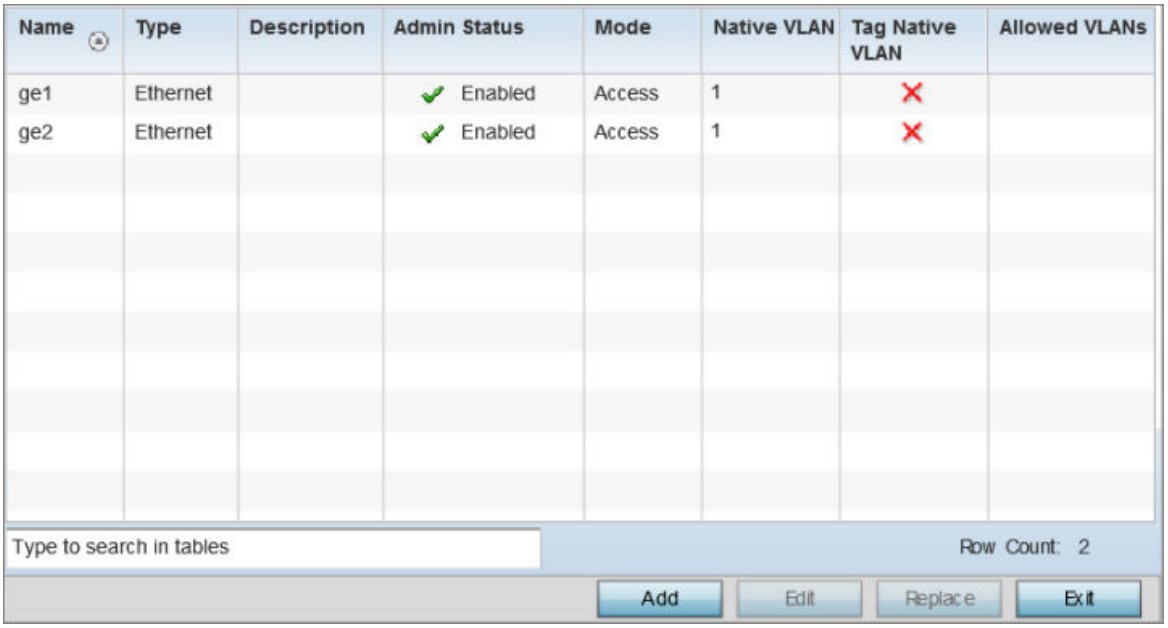



**Figure 26: Device Configuration - System Profile - Interfaces - Ethernet Ports screen**

3 Refer to the following to assess port status, mode and VLAN configuration:

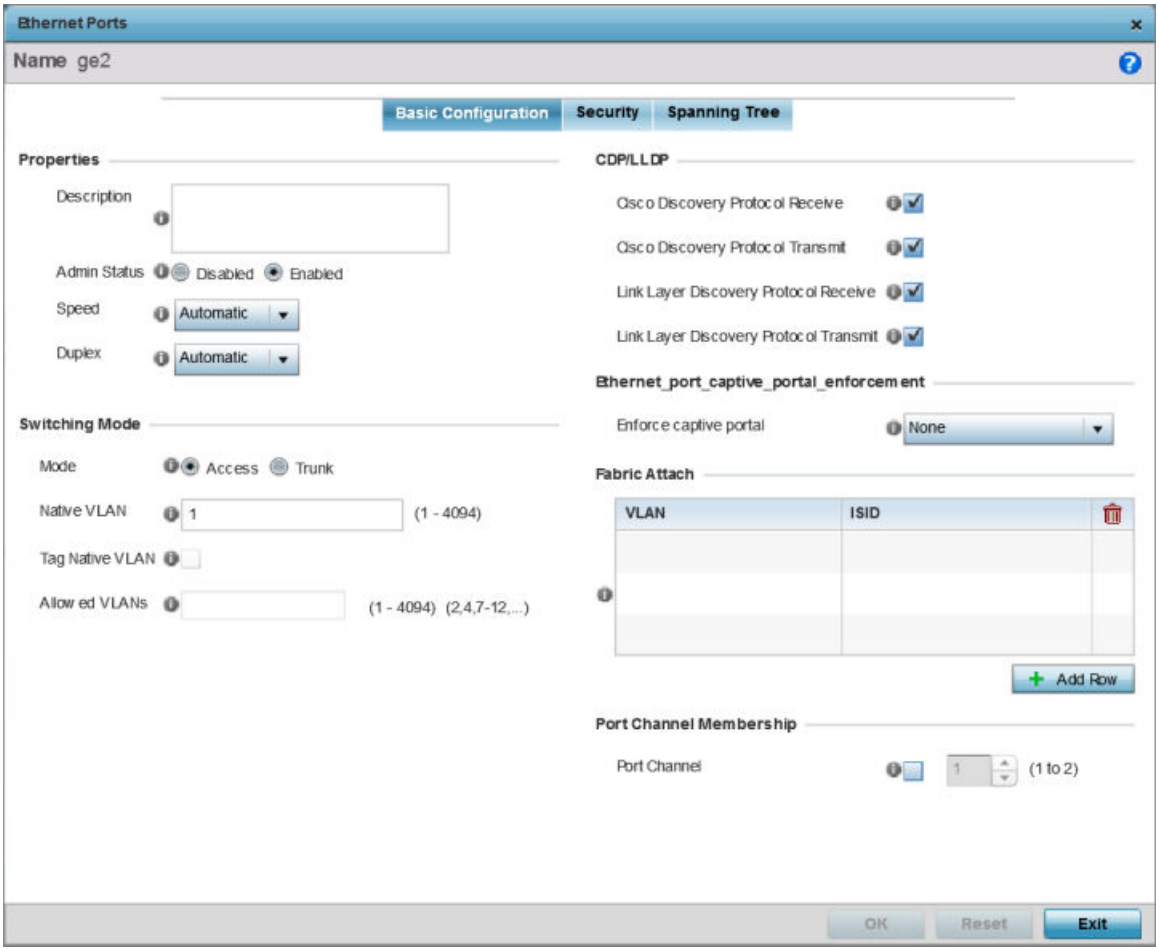
| | |
|---|---|
| Name | Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on model. |
| Type | Displays the physical port type. |
| Description | Displays an administrator defined description for each listed port. |
| Admin Status | A green check mark means the port is active and currently enabled with the profile. A red "X" means the port is currently disabled and not available for use. The interface status can be modified with the port configuration as needed. |
| Mode | The profile's switching mode: either **`Access`** or **`Trunk`** (as defined on the Ethernet Port Basic Configuration screen).<br>If **`Access`** is selected, the port accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN.<br>If **`Trunk`** is selected, the port allows packets from a list of VLANs added to the trunk. The port supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged. |

| | |
|---|---|
| Native VLAN | The VLAN ID (1 - 4094) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN over which untagged traffic is directed when using a port in **Trunk** mode. |
| Tag Native VLAN | A green check mark means the native VLAN is tagged. A red "X" means the native VLAN is untagged.<br>When a frame is tagged, the 12-bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12-bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. |
| Allowed VLANs | The VLANs allowed to send packets over the listed port. Allowed VLANs are listed only when the port is in **Trunk** mode. |

### Basic Ethernet Port Configuration

To define a profile's Ethernet port basic configuration:

1 To edit the configuration of an existing port, select it from amongst those displayed and select the **Edit** button. The Ethernet port **Basic Configuration** screen displays by default.




2 Set the following Ethernet port Properties:

| | |
|---|---|
| Description | Enter a brief description for the port (64 characters maximum). The description should reflect the port's intended function to differentiate it from others with similar configurations or perhaps just the name of the physical port. |
| Admin Status | Select the **Enabled** radio button to define this port as active to the controller profile it supports. Select the **Disabled** radio button to disable this physical port in the profile. It can be activated at any future time when needed. |

| | |
|---|---|
| Speed | Select the speed at which the port can receive and transmit the data. Select either **`10 Mbps`**, **`100 Mbps`** or **`1000 Mbps`**. Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select **`Automatic`** to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. *Automatic* is the default setting. |
| Duplex | Select either **`half`**, **`full`** or **`automatic`** as the duplex option. Select *Half* duplex to send data over the port, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time. Select *Full* duplex to transmit data to and from the device port at the same time. Using Full duplex, the port can send data while receiving data as well. Select *Automatic* to dynamically duplex as port performance needs dictate. Automatic is the default setting. |

3 Enable or disable the following CDP/LLDP parameters used to configure *Cisco Discovery Protocol* and *Link Layer Discovery Protocol* for this profile's Ethernet port configuration:

| | |
|---|---|
| Cisco Discovery Protocol Receive | Select this box to allow the Cisco discovery protocol to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default. |
| Cisco Discovery Protocol Transmit | Select this box to allow the Cisco discovery protocol to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. |
| Link Layer Discovery Protocol Receive | Select this box to allow the Link Layer discovery protocol to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default. |
| Link Layer Discovery Protocol Transmit | Select this box to allow the Link Layer discovery protocol to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. |

4 Set the following Power Over Ethernet (PoE) parameters for this profile's Ethernet port configuration:

| | |
|---|---|
| Enable POE | Select the check box to configure the selected port to use Power over Ethernet. To disable PoE on a port, clear this option. Power over Ethernet is supported on RFS 4000 model controllers only. When enabled, the controller supports 802.3af PoE on each of its ge ports. The PoE allows users to monitor port power consumption and configure power usage limits and priorities for each ge port. |
| Power Limit | Use the spinner control to set the total watts available for Power over Ethernet on the defined ge port. Set a value between 0 - 40 watts. |
| Power Priority | Set the power priority for the listed port to either to either *Low*, *Medium* or *High*. This is the priory assigned to this port versus the power requirements of the other ports on the controller. |

5 Define the following **Switching Mode** parameters to apply to the Ethernet port configuration:

| | |
|---|---|
| Mode | Select either the **Access** or **Trunk** radio button to set the VLAN switching mode over the port. If Access is selected, the port accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port allows packets from a list of VLANs you add to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default mode. |
| Native VLAN | Use the spinner control to define a numerical *Native VLAN ID* between 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1. |
| Tag Native VLAN | Select the check box to tag the native VLAN. WiNG managed devices support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default. |
| Allowed VLANs | Selecting Trunk switching mode enables the *Allowed VLANs* parameter to add VLANs that exclusively send packets over the listed port. |

6 In the Dynamic Link Aggregation (LACP) area, set the following parameters to enable link aggregation on the selected GE port:

| | |
|---|---|
| Port Channel | Select to configure the selected port as a member of a LAG *(link aggregation group)*. Link aggregation is supported only on the following platforms: AP7502, AP7602, AP7612, AP8432, AP8533, NX5500, NX7500, NX9500, NX9600, and VX900.<br>LACP enables combining and managing multiple physical connections like Ethernet ports as a single logical channel as defined in the IEEE 802.1ax standard. LACP provides redundancy and increase in throughput for connections between two peers. It also provides automatic recovery in cases where one or more of the physical links - making up the aggregation - fail. Similarly, LACP also provides a theoretical boost in speed compared to an individual physical link.<br><br>Note: if enabling LACP, disable or physically disconnect interfaces that do not use spanning tree to prevent loop formation until LACP is fully configured on both the local WiNG device and the remote device. |
| Port Mode | Set the port mode as **Active** or **Passive**. If setting the port as a LAG member, specify whether the port is an active or passive member within the group.<br>An active member initiates and participates in LACP negotiations. It is the active port that always transmits LACPDU irrespective of the remote device's port mode.<br>The passive port only responds to LACPDU received from its corresponding active port.<br>At least one port within a LAG, on either of the two negotiating peers, should be in the active mode. LACP negotiations are not initiated if all LAG member ports are passive. Further, the peer-to-peer LACP negotiations are always initiated by the peer with the lower system-priority value. |
| Port Priority | Select this check box and set the selected Ethernet Port's priority value, within the LAG, from 1-65535.<br>The selected port's actual priority within the LAG is determined by the port-priority value specified here along with the port's number. Higher the value, lower is the priority. Use this option to manipulate a port's priority. For example, in a LAG having five physical ports, four active and one standby, manually increasing the standby port's priority ensures that if one of the active port fails, the standby port is included in the LAG during re-negotiation. |

7 Select a Captive Portal Enforcement option for the selected Ethernet port interface.

Captive portal enforcement allows wired network users to pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user can pass traffic on the captive portal. If **None** is selected, captive portal policies are not enforced on the wired interface. If **Authentication Failure** is selected, captive portal policies are enforced only when RADIUS authentication of the client's MAC address is not successful. If **Always** is selected, captive portal policies are enforced regardless of whether the client's MAC address is in the RADIUS server's user database.

8 Click **+ Add Row** and set or override the Fabric Attach parameters. This option enables WiNG devices (access points and controllers) as FA *(Fabric Attach)* Clients.

Note
To enable FA Client feature, the Ethernet port's switching mode should be set to trunk.

| | |
|---|---|
| VLAN | Set the VLAN from 1 - 4094. |
| ISID | User the spinner control to specify the ISID from 1 - 16777214. This is the ISID *(Individual Service Identifier)* associated with the VLAN interface specified above.<br>Configuring a VLAN to ISID assignment, enables FA client operation on the selected Ethernet port.<br>The FA Client requests acceptance of the VLAN to ISID mapping from the FAS within the FC *(Fabric Connect)* network. Once acceptance is achieved, the FC edge switch applies the ISID to the VLAN traffic from the device (AP or controller), and uses this ISID inside the Fabric.<br><br>Note: A maximum of 94 pairs of I-SID to VLAN mappings can be configured per Ethernet port. |

FA-enabled switches, in the FC network, send out LLDP messages with TLV extensions of Organization-specific TLV with OUI, to discover FA clients and advertise capabilities.

The FA-enabled client associates with the FAS *(FA Server)*, and obtains provisioning information (management VLAN interface details, and whether the interface is tagged or not) that allows the client to be configured with parameters that allow traffic to flow through the Fabric to the WLAN controller. Use this option to configure the ISID to VLAN mapping that the FA Client uses to negotiate with the FAS.

You can configure FA Client capability on a device's profile as well as device contexts.

9 Optionally select the **Port Channel** checkbox and define a setting between 1 - 3 using the spinner control. This sets the channel group for the port.

10 Select **OK** to save the changes made to the Ethernet Port Basic Configuration. Select **Reset** to revert to the last saved configuration.

### Ethernet Port Security Configuration

To define a profile's Ethernet port security configuration:

1 Select the **Security** tab.

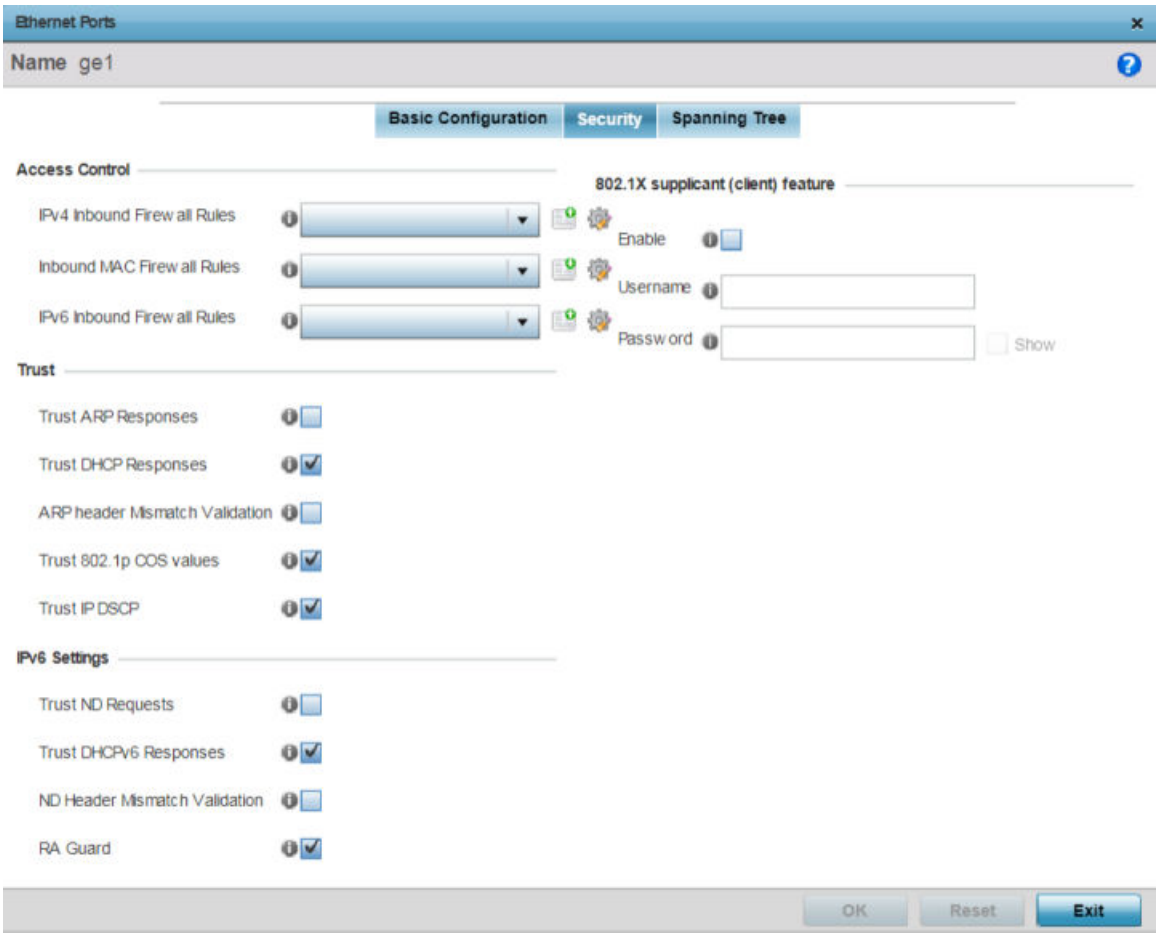



**Figure 27: Interface GE Port - Security Tab**

2 Refer to the **Access Control** field. As part of the port's security configuration, Inbound IP and MAC address firewall rules are required.

Use the **Inbound IP Firewall Rules** and **MAC Inbound Firewall Rules** pull-down menus to select the firewall rules to apply to this profile's Ethernet port configuration.

The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

3 If a firewall rule does not exist suiting the data protection needs of the target port configuration, select the **Create** icon to define a new rule configuration. For more information, see Wireless Firewall on page 730.

4 Refer to the **Trust** field to define the following:

| | |
|---|---|
| Trust ARP Responses | Select the check box to enable ARP trust on this port. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled. |
| Trust DHCP Responses | Select the check box to enable DHCP trust on this port. If enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled. |

| | |
|---|---|
| ARP header Mismatch Validation | Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is disabled. |
| Trust 802.1p COS values | Select the check box to enable 802.1p COS values on this port. The default value is enabled. |
| Trust IP DSCP | Select the check box to enable IP DSCP values on this port. The default value is enabled.<br><br>Note: Some vendor solutions with VRRP enabled send ARP packets with Ethernet SMAC as a physical MAC and inner ARP SMAC as VRRP MAC. If this configuration is enabled, a packet is allowed, despite a conflict existing. |

5 Set the following **IPv6 Settings**

| | |
|---|---|
| Trust ND Requests | Select this option to enable the trust of neighbor discovery requests required on an IPv6 network on this Ethernet port. This option is disabled by default. |
| Trust DHCPv6 Responses | Select this option to trust all DHCPv6 responses on this Ethernet port. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network. This option is enabled by default. |
| ND Header Mismatch Validation | Select this option to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This option is disabled by default. |
| RA Guard | Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This option is enabled by default. |

6 Set the following **802.1X Settings**:

| | |
|---|---|
| Host Mode | Use the drop-down menu to select the host mode configuration to apply to this port. Options include *single-host* or *multi-host.* The default setting is single-host. |
| Guest VLAN | Specify a guest VLAN for this port from 1 - 4094. This is the VLAN traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled. |
| Port Control | Use the drop-down menu to set the port control state to apply to this port. Options include *force-authorized*, *force-unauthorized* and *automatic*. The default setting is force-authorized. |
| Re Authenticate | Select this setting to force clients to reauthenticate on this port. The default setting is disabled, thus clients do not need to reauthenticate for connection over this port until this setting is enabled. |
| Max Reauthenticate Count | Set the maximum reauthentication attempts (1 - 10) before this port is moved to unauthorized. The default setting is 2. |
| Maximum Request | Set the maximum number of authentication requests (1 - 10) before returning a failed message to the requesting client. The default setting is 2. |
| Quiet Period | Set the quiet period for this port from 1 - 65,535 seconds. This is the maximum wait time 802.1x waits upon a failed authentication attempt. The default setting is 60 seconds. |

| | |
|---|---|
| Reauthenticate Period | Use the spinner control to set the reauthentication period for this port from 1 - 65,535 seconds. The default setting is 60 seconds. |
| Port MAC Authentication | When enabled, a port's MAC address is authenticated, as only one MAC address is supported per wired port. When successfully authenticated, packets from the source are processed. Packets from all other sources are dropped. Port MAC authentication is supported on RFS 4000, model controllers and NX 9000 series service platforms.<br>Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy. |

7 Select **Enable** within the 802.1x supplicant (client) field to enable a username and password pair used when authenticating users on this port. This setting is disabled by default. The password cannot exceed 32 characters.

8 Select **OK** to save the changes made to the Ethernet port's security configuration. Select **Reset** to revert to the last saved configuration.

### Spanning Tree Configuration

To define an Ethernet port's spanning tree configuration:

1 Select **Configuration → Devices → System Profile**.

The Profile screen, listing device profiles is displayed.

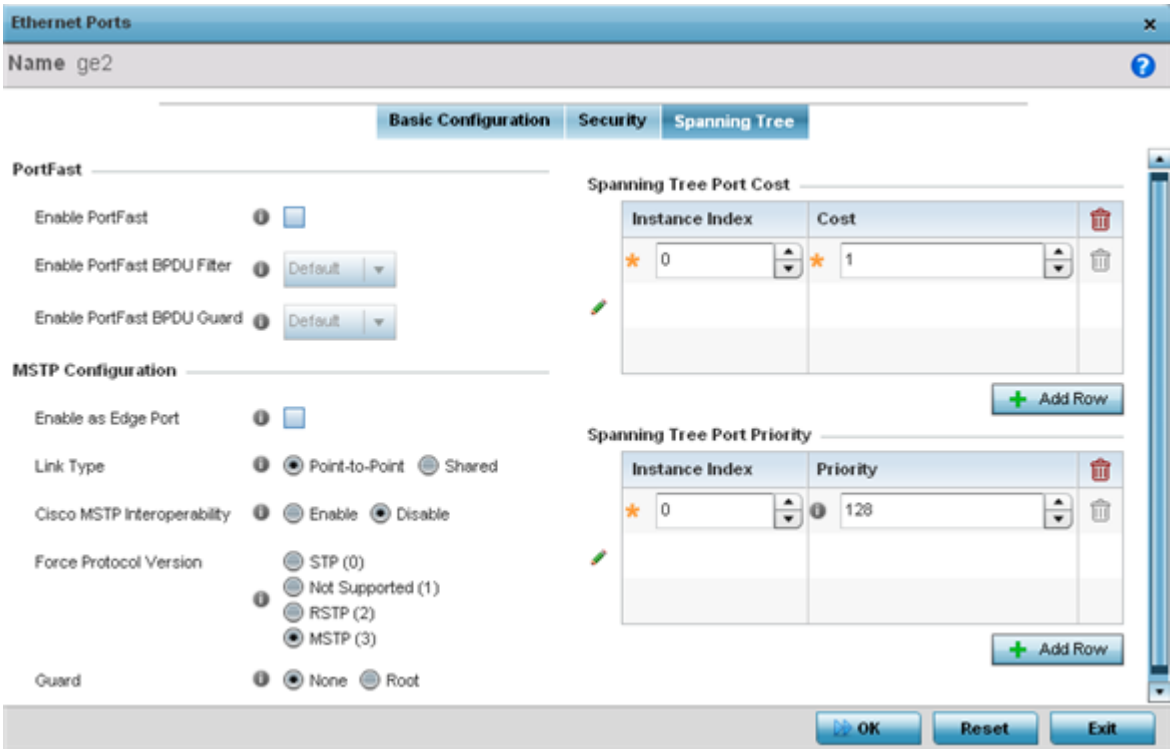
2 Select a device profile from those listed on the screen.

The selected device profile's configuration menu displays.

3 Expand the **Interface** menu and select **Ethernet Ports**.

4 To edit the configuration of an existing port, select it from amongst those displayed and select the **Edit** button.

5 Select the **Spanning Tree** tab.




6 Define the following **PortFast** parameters for the port's MSTP configuration:

| | |
|---|---|
| Enable PortFast | Select the check box to enable pull-down menus for both the Enable Portfast BPDU Filter and Enable Portfast BPDU guard options for the port. |
| PortFast BPDU Filter | Select enable to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this PortFast enabled port does not transmit or receive BPDUs. |
| PortFast BPDU Guard | Select enable to invoke a BPDU guard for this portfast enabled port. Enabling the BPDU Guard feature means this portfast-enabled port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. |

7 Set the following **MSTP Configuration** parameters:

| | |
|---|---|
| Enable as Edge Port | Select the check box to define this port as an edge port. Using an edge (private) port, isolate devices to prevent connectivity over this port. |
| Link Type | Select either the **Point-to-Point** or **Shared** radio button. Selecting Point-to-Point indicates the port should be treated as connected to a point-to-point link. Selecting Shared indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one the connected to a controller is a point-to-point link. |
| Cisco MSTP Interoperability | Select either the **Enable** or **Disable** radio buttons. This enables interoperability with Cisco's version of MSTP over the port, which is incompatible with standard MSTP. |

| | |
|---|---|
| Force Protocol Version | Sets the protocol version to either **STP(0)**, **Not Supported(1)**, **RSTP(2)** or **MSTP(3)**. MSTP is the default setting. |
| Guard | Determines whether the port enforces root bridge placement. Setting the guard to *Root* ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position. |

8 Refer to the **Spanning Tree Port Cost** table.

9 Define an **Instance Index** using the spinner control, then set the **Cost**. The default path cost depends on the speed of the port. The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

| Speed | Default Path Cost |
|---|---|
| <=100000 bits/sec | 200000000 |
| <=1000000 bits/sec | 20000000 |
| <=10000000 bits/sec | 2000000 |
| <=100000000 bits/sec | 200000 |
| <=1000000000 bits/sec | 20000 |
| <=10000000000 bits/sec | 2000 |
| <=100000000000 bits/sec | 200 |
| <=1000000000000 bits/sec | 20 |
| >1000000000000 bits/sec | 2 |

10 Select **+ AddRow** as needed to include additional indexes.

11 Refer to the **Spanning Tree Port Priority** table.

Define an **Instance Index** using the spinner control and assign a **Priority** value. The lower the priority, a greater likelihood of the port becoming a designated port. Thus applying an higher value impacts the port's likelihood of becoming a designated port.

12 Select **+ Add Row** needed to include additional indexes.

13 Select **OK** to save the changes made to the Ethernet Port's spanning tree configuration. Select **Reset** to revert to the last saved configuration.

### *Virtual Interface Configuration*

A virtual interface is required for layer 3 (IP) access to a controller or service platform or provide to layer 3 service on a VLAN. The virtual interface defines which IP address is associated with each VLAN ID the controller or service platform is connected to. A virtual interface is created for the default VLAN (VLAN 1) to enable remote administration. A virtual interface is also used to map VLANs to IP address ranges. This mapping determines the destination for routing.

To review existing virtual interface configurations and create a new virtual interface configuration, modify (override) an existing configuration or delete an existing configuration:

1 Select **Configuration → Devices → System Profile** from the web UI.

A list of device profiles is displayed in the right-hand UI. This list contains default and user-defined profiles.

2 Select a profile from those listed on the screen.

The profile's configuration menu is displayed.

3 Expand the **Interface** menu and select **Virtual Interfaces**.

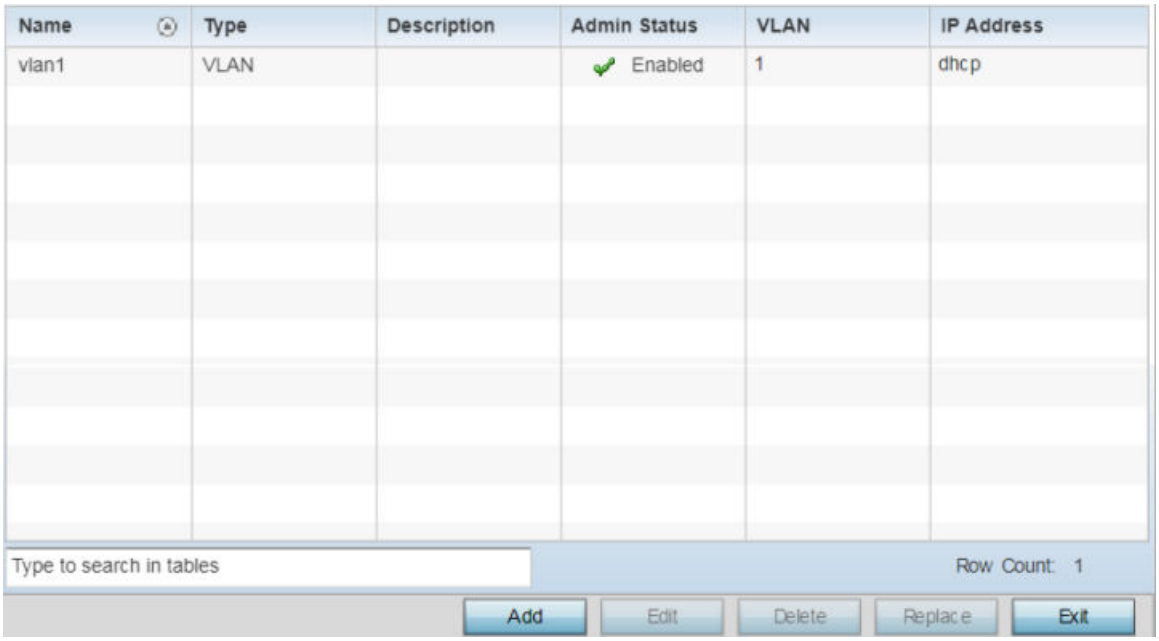



**Figure 28: Profile Interface - Virtual Interfaces screen**

4 Review the following parameters unique to each virtual interface configuration:

| | |
|---|---|
| Name | The name of each listed virtual interface assigned when it was created. The name is between 1 - 4094, and cannot be modified as part of a virtual interface edit. |
| Type | The type of virtual interface for each listed interface. |
| Description | The description defined for the virtual interface, either when it was created or when it was edited. |
| Admin Status | A green check mark means the listed virtual interface configuration is active and enabled with its supported profile. A red "X" means the virtual interface is currently shut down. The interface status can be modified when a new virtual interface is created or an existing one modified. |
| VLAN | The numerical VLAN ID associated with each listed interface. |
| IP Address | Whether DHCP was used to obtain the primary IP address used by the virtual interface configuration. |

After reviewing the configurations of existing virtual interfaces, determine whether a new interface needs to be created, an existing virtual interface needs to be edited (overridden), or an existing virtual interface needs to be deleted.

### General Configuration

To configure the VLAN's basic configurations:

1 Select **Add** to define a new virtual interface configuration, **Edit** to modify or override the configuration of an existing virtual interface, or **Delete** to permanently remove a selected virtual interface.

The Basic Configuration screen displays by default, regardless of a whether a new virtual interface is being created or an existing one is being modified. Select the **General** tab if it is not selected by default.

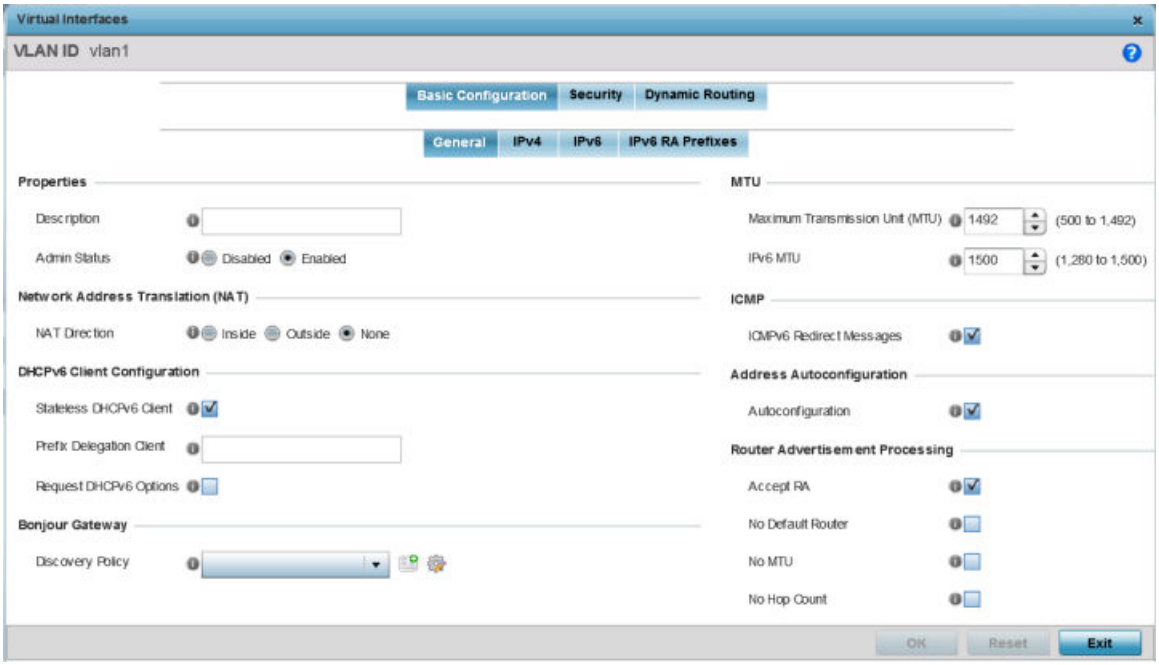



**Figure 29: Profile Overrides - Virtual Interfaces Basic Configuration Screen**

2 If you are creating a new virtual interface, use the **VLAN ID** spinner control to define a numeric VLAN ID from 1 - 4094.

3 Define or override the following parameters in the Properties field:

| | |
|---|---|
| Description | Provide or edit a description (up to 64 characters) for the virtual interface that helps differentiate it from others with similar configurations. |
| Admin Status | Select **Disabled** or **Enabled** to define this interface's current status within the managed network. When set to **Enabled**, the virtual interface is operational and available to the controller or service platform. The default value is enabled. |

4 Define or override the Network Address Translation (NAT) direction.

Select one of the following options:

Inside The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.

Outside Packets passing through the NAT on the way back to the managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the switch managed network.

None No NAT activity takes place. This is the default setting.

5 Set the following **DHCPv6 Client Configuration**.

The DHCPv6 *(Dynamic Host Configuration Protocol for IPv6)* provides a framework for passing configuration information.

| | |
|---|---|
| Stateless DHCPv6 Client | Select this option to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default. |
| Prefix Delegation Client | Specify a 32-character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface. Devices use prefixes to distinguish destinations that reside on-link from those reachable using a router. |
| Request DHCPv6 Options | Select this option to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than locally. This setting is disabled by default. |

6 Define the **Bonjour Gateway** settings.

Bonjour is Apple's implementation of zeroconfiguration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers, and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a *local area network* (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

Select the **Bonjour Gateway Discover** policy from the drop-down menu. Click the **Create** icon to define a new Bonjour Gateway policy configuration, or click the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

7 Define the following **MTU** settings for the virtual interface:

| | |
|---|---|
| Maximum Transmission Unit (MTU) | Set the PPPoE client MTU from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492. |
| IPv6 MTU | Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500. |

8 In the **ICMP** field, define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route.

This setting is enabled by default.

9 In the Address Autoconfiguration field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits.

This setting is enabled by default.

10 Set the following Router Advertisement Processing settings for the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

| | |
|---|---|
| Accept RA | Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.This setting is enabled by default. |
| No Default Router | Select this option to consider routers unavailable on this interface for default router selection. This setting is disabled by default. |
| No MTU | Select this option to not use the existing MTU setting for router advertisements on this virtual interface. If the value is set to zero, no MTU options are sent. This setting is disabled by default. |
| No Hop Count | Select this option to not use the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default. |

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

Click **Reset** to revert to the last saved configuration.

### IPv4 Configuration

IPv4 is a connectionless protocol. It operates on a best effort delivery model that does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

To configure the VLAN IPv4 configuration:

1 Select the **IPv4** tab.

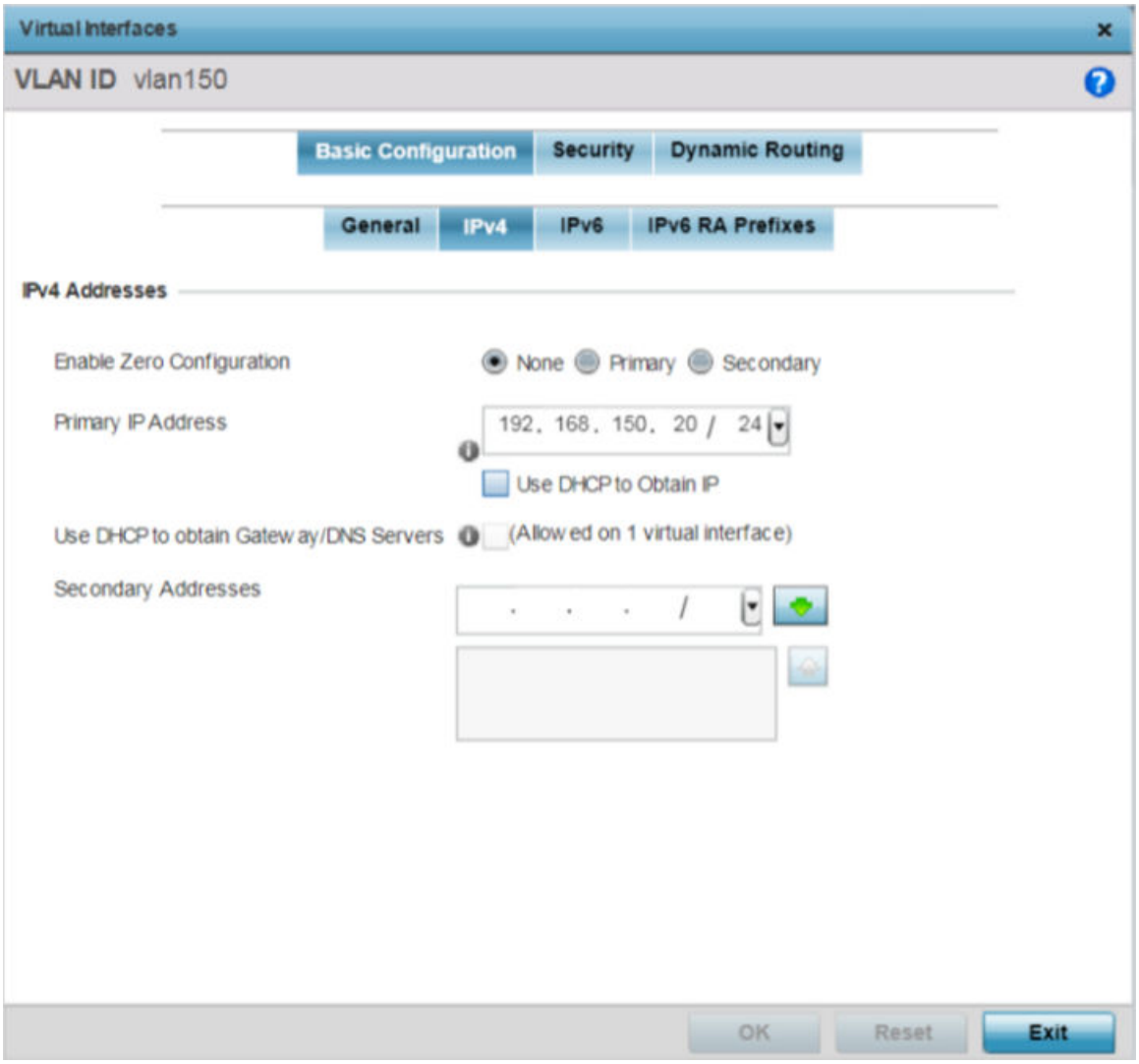



**Figure 30: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv4 Tab**

2 Set the following network information in the IPv4 Addresses field:

| | |
|---|---|
| Enable Zero Configuration | Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to None by default. |
| Primary IP Address | Define the IP address for the VLAN associated virtual interface. |
| Use DHCP to Obtain IP | Select this option to allow DHCP to provide the IP address for the virtual interface. Selecting this option disables the Primary IP Address field. |

| | |
|---|---|
| Use DHCP to Obtain Gateway/DNS Servers | Select this option to allow DHCP to obtain a default gateway address and DNS resource for one virtual interface. This setting is disabled by default and only available when the **Use DHCP to Obtain IP** option is selected. |
| Secondary Addresses | Use this parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable. |

3 Click **OK** to save the changes to the IPv4 configuration.

Click **Reset** to revert to the last saved configuration.

### IPv6 Configuration

IPv6 is the latest revision of the IP *(Internet Protocol)*, designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

To configure the VLAN IPv6 configuration:

1 Select the **IPv6** tab.

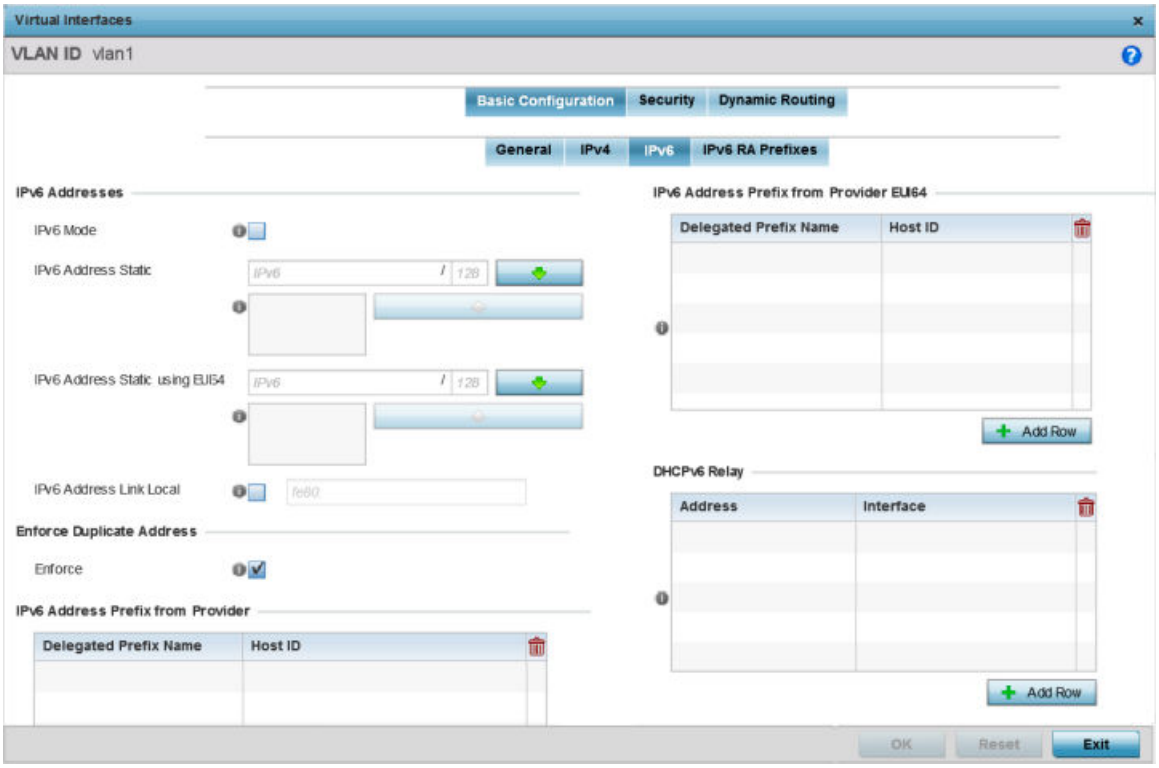



**Figure 31: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab**

2 Refer to the IPv6 Addresses field to define how IP6 addresses are created and utilized:

| | |
|---|---|
| IPv6 Mode | Select this option to enable IPv6 support on this virtual interface. IPv6 is disabled by default. |
| IPv6 Address Static | Define up to 15 global IPv6 IP addresses that can created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons. |
| IPv6 Address Static using EUI64 | Optionally, set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24- bits, with one being an OUI *(Organizationally Unique Identifier)* and the other being client specific. A 16-bit 0xFFFE is then inserted between the two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address. |
| IPv6 Address Link Local | Provide the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled, even when one or more routable addresses are assigned. |

3 Enable the Enforce Duplicate Address option to enforce duplicate address protection when any wired port is connected and in a forwarding state.

This option is enabled by default.

4 Refer to the IPv6 Address Prefix from Provider table to create IPv6 format prefix shortcuts as supplied by an ISP.

Select **+ Add Row** to launch a screen in which a new delegated prefix name and host ID can be defined.

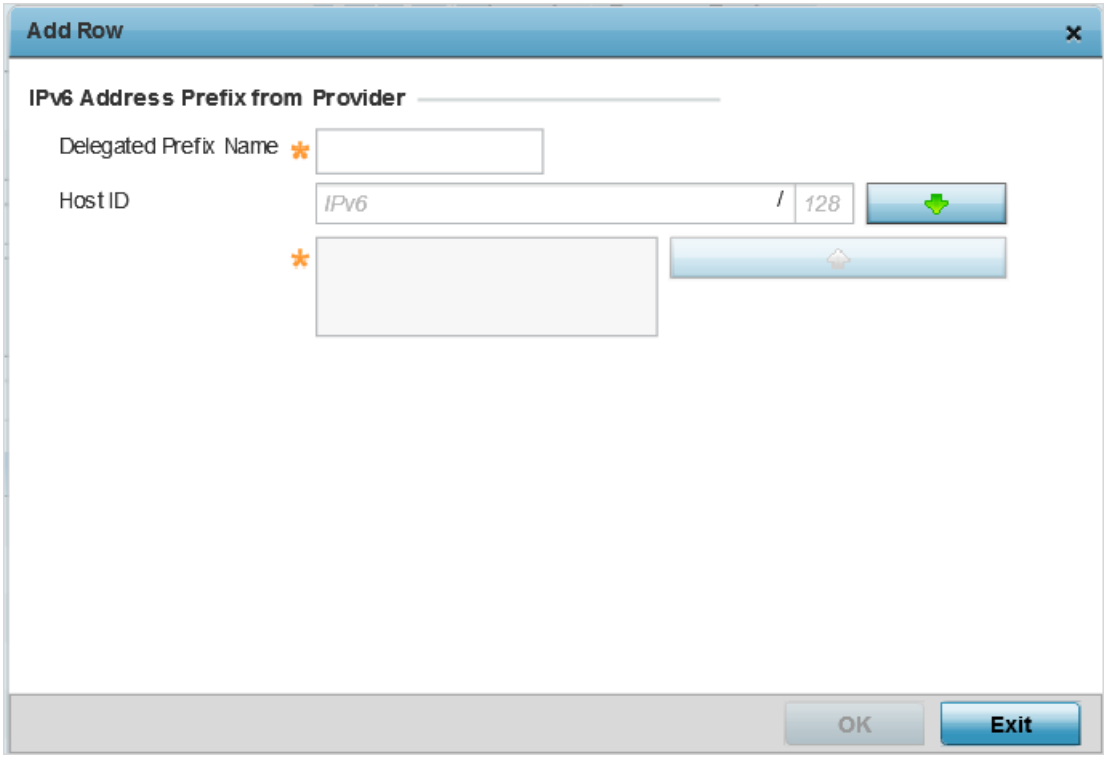



**Figure 32: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider**

| | |
|---|---|
| Designated Prefix Name | Enter a 32-character maximum name for the IPv6 address prefix from your provider. |
| Host ID | Define the subnet ID, host ID, and prefix length. |

5 Click **OK** to save the changes to the IPv6 configuration.

Click **Exit** to close the screen without saving any updates.

6 Refer to the IPv6 Address Prefix from Provider EUI64 table to set an (abbreviated) IP address prefix in EUI64 format.

Select **+ Add Row** to launch a screen in which a new delegated prefix name and host ID can be defined in EUI64 format.

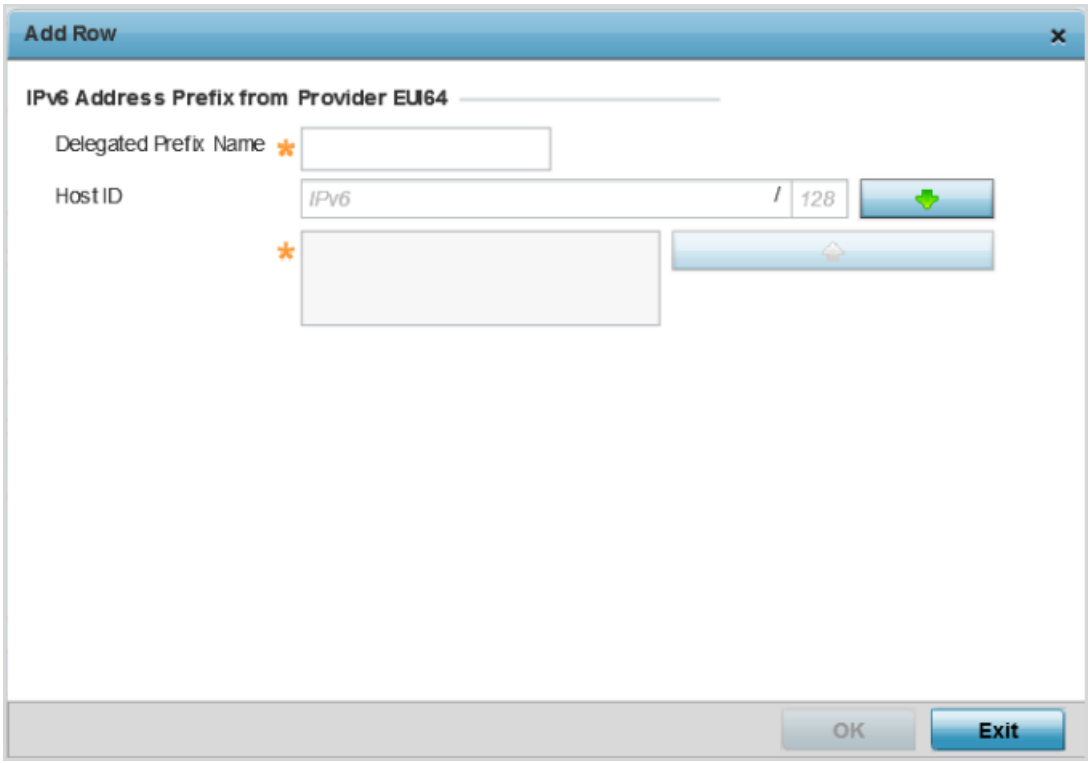



**Figure 33: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider EUI64**

| | |
|---|---|
| Designated Prefix Name | Enter a 32-character maximum name for the IPv6 prefix from your provider in EUI format. Using EUI64, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without manual configuration or DHCP. |
| Host ID | Define the subnet ID and prefix length. |

7 Click **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format.

Click **Exit** to close the screen without saving any updates.

8 Refer to the DHCPv6 Relay table to set the address and interface of the DHCPv6 relay.

The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent

forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

Select **+ Add Row** to launch a screen in which a new DHCPv6 relay address and interface VLAN ID can be set.

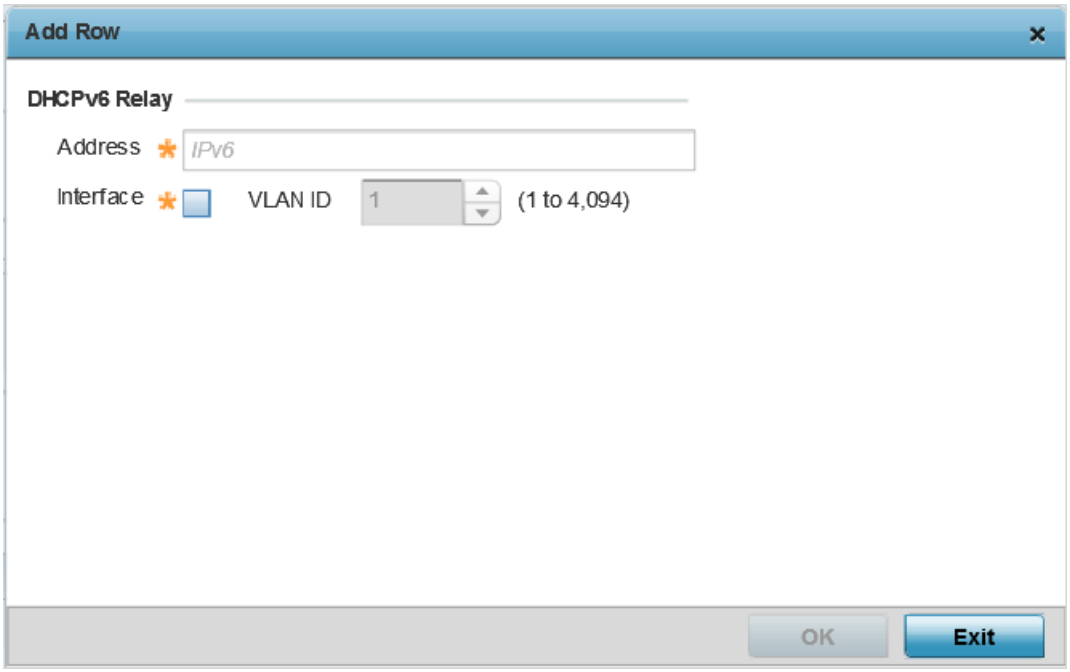



**Figure 34: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add DHCPv6 Relay**

| | |
|---|---|
| Address | Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network. |
| Interface | Select this option to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available. |

9 Click **OK** to save the changes to the DHCPv6 relay configuration.

Click **Exit** to close the screen without saving any updates.

### IPv6 RA Prefixes Configuration

To configure the VLAN IPv6 RA Prefixes configuration:

1 Select the **IPv6 RA Prefixes** tab.

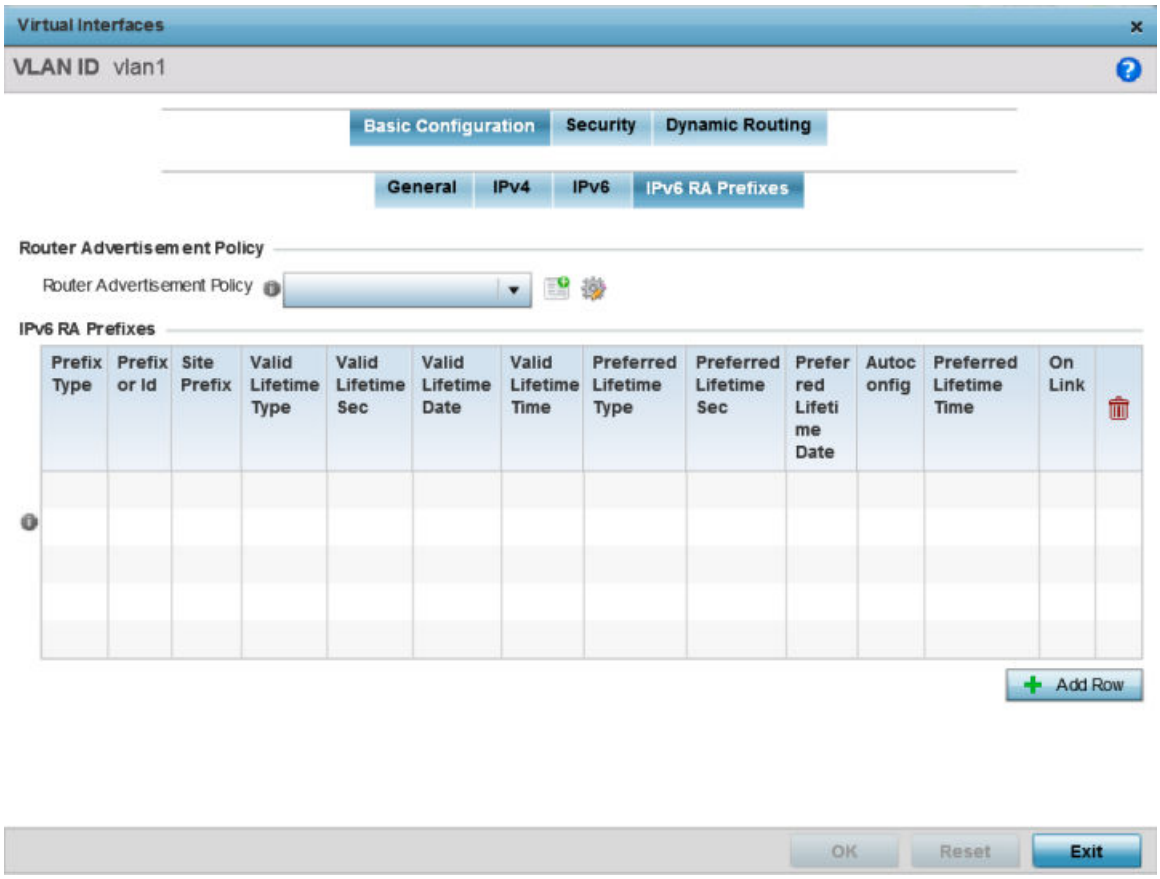



**Figure 35: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefixes Tab**

2 Use the **Router Advertisement Policy** drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

3 Review the configurations of existing IPv6 advertisement policies.

If necessary, select **+ Add Row** to define the configuration for an additional IPv6 RA prefix.

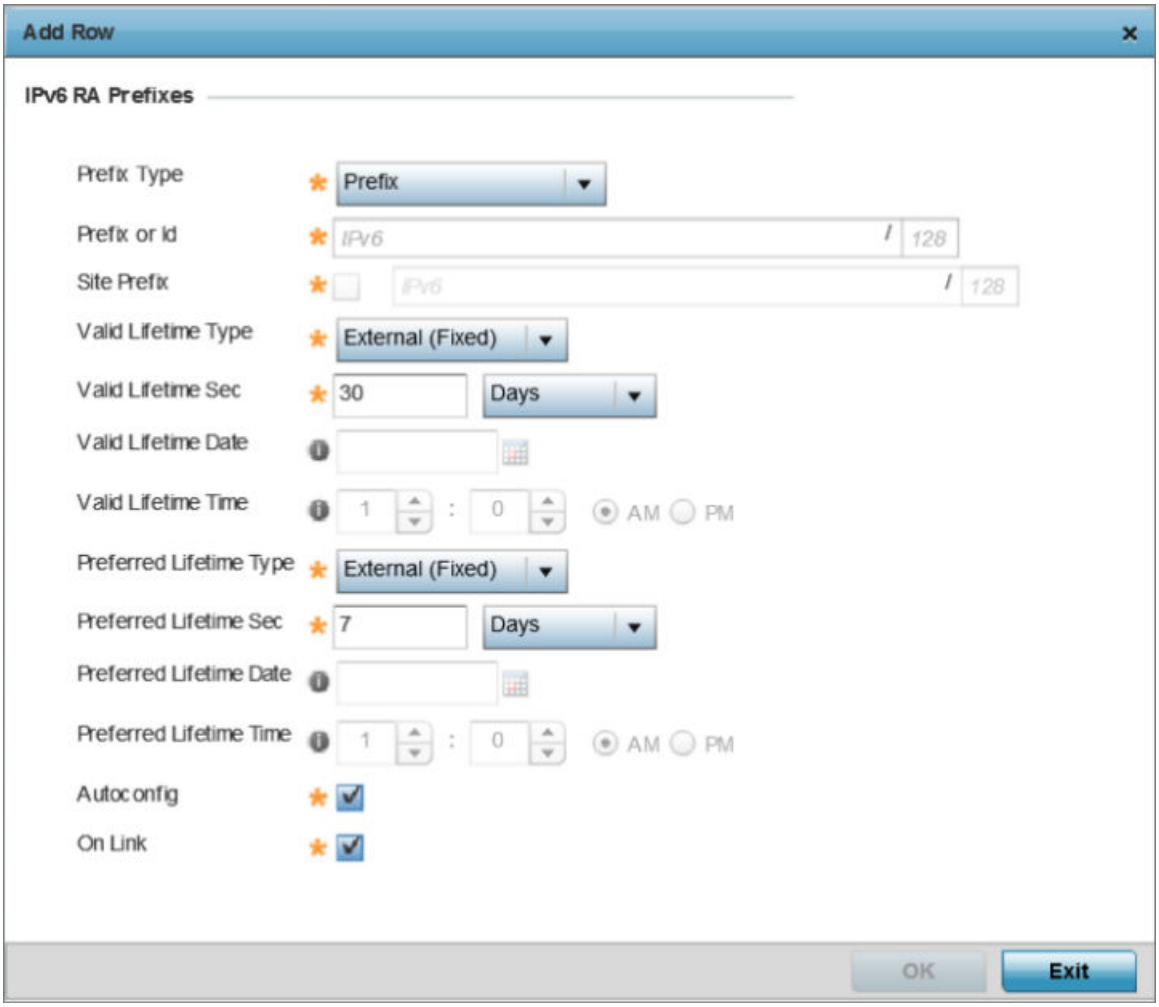



**Figure 36: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefix**

4 Define the following IPv6 RA Prefix settings:

| | |
|---|---|
| Prefix Type | Set the prefix delegation type used with this configuration. Options include **`Prefix`**, and **`prefix-from-provider`**. The default setting is **`Prefix`**. A prefix allows an administrator to associate a user defined name to an IPv6 prefix. A provider assigned prefix is made available from an ISP *(Internet Service Provider)* to automate the process of providing and informing the prefixes used. |
| Prefix or ID | Set the actual prefix or ID used with the IPv6 router advertisement. |
| Site Prefix | The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link. |

| | |
|---|---|
| Valid Lifetime Type | Set the lifetime for the prefix's validity. Options include **External** (fixed), **decrementing,** and **infinite**. If set to **External** (fixed), only the **Valid Lifetime Sec** setting is enabled to define the exact time interval for prefix validity. If set to **decrementing,**, use the lifetime date and time settings to refine the prefix expiry period. If set to **infinite**, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is **External** (fixed). |
| Valid Lifetime Sec | If the lifetime type is set to **External** (fixed), set the Seconds, Minutes, Hours, or Days values used to measure the prefix's expiration. 30 days, 0 hours, 0 minutes, and 0 seconds is the default lifetime. |
| Valid Lifetime Date | If the lifetime type is set to **External** (fixed), set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Valid Lifetime Time | If the lifetime type is set to **decrementing**, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the **AM** and **PM** radio buttons to set the appropriate hour. |
| Preferred Lifetime Type | Set the administrator preferred lifetime for the prefix's validity. Options include **External** (fixed), **decrementing,** and **infinite**. If set to **External** (fixed), only the **Preferred Lifetime Sec** setting is enabled to define the exact time interval for prefix validity. If set to **decrementing,**, use the lifetime date and time settings to refine the prefix expiry period. If set to **infinite**, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is **External** (fixed). |
| Preferred Lifetime Sec | If the administrator preferred lifetime type is set to **External** (fixed), set the Seconds, Minutes, Hours, or Days values used to measure the prefix's expiration. 30 days, 0 hours, 0 minutes, and 0 seconds is the default lifetime. |
| Preferred Lifetime Date | If the administrator preferred lifetime type is set to **External** (fixed), set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Preferred Lifetime Time | If the administrator preferred lifetime type is set to **decrementing**, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the **AM** and **PM** radio buttons to set the appropriate hour. |
| Autoconfig | Autoconfiguration includes generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default. |
| On Link | Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled. |

5 Click **OK** to save the changes to the IPv6 RA prefix configuration.

Click **Exit** to close the screen without saving any updates. Or, click **Reset** to revert to the last saved configuration.

### Security Configuration

Use this screen to configure firewalls. The firewall inspects packet traffic to and from connected clients. If there is no firewall rule that meets the data protection needs of this virtual interface, select the **Create** icon to define a new firewall rule configuration or the **Edit** icon to modify or override an existing configuration. For more information, see Wireless Firewall on page 730.

To set the VLAN security configuration:

1 Select the **Security** tab.

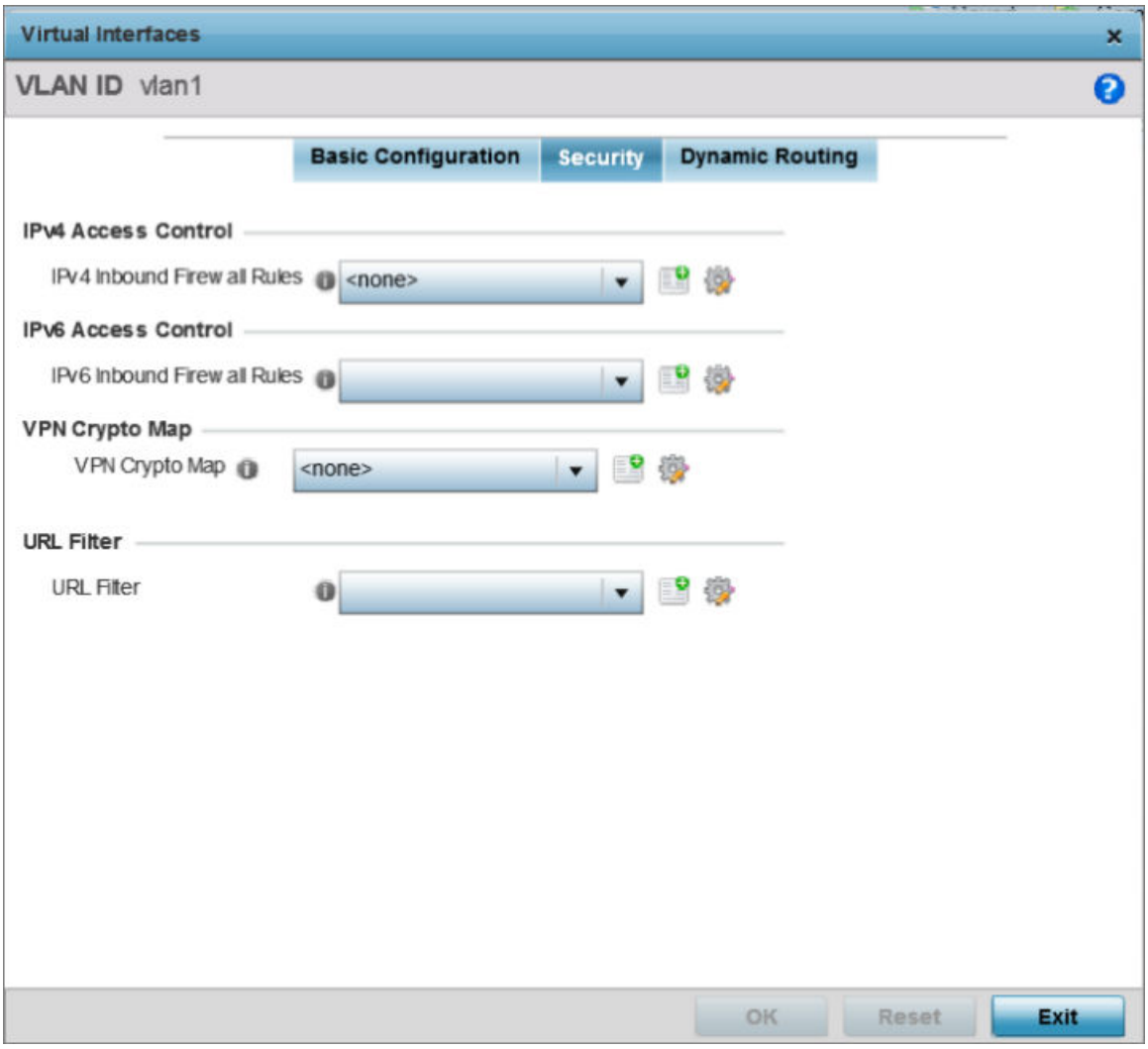



**Figure 37: Profile Overrides - Virtual Interfaces Security Screen**

2 Use the **IPv4 Inbound Firewall Rules** drop-down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration.

Click the **Create** icon to define a new IPv4 firewall rule configuration, or click the **Edit** icon to modify an existing configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, since it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). For more information on creating IPv4 firewall rules, see Configuring IP Firewall Rules on page 744.

IPv4 and IPv6 are different enough to warrant separate protocols. IPv6 devices can alternatively use stateless address autoconfiguration. IPv4 hosts can use link local addressing to provide local connectivity.

3 Use the **IPv6 Inbound Firewall Rules** drop-down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration.

Click the **Create** icon to define a new IPv6 firewall rule configuration, or click the **Edit** icon to modify an existing configuration.

IPv6 is the latest revision of the IP *(Internet Protocol)* replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. For more information on creating IPv6 firewall rules, see Configuring IP Firewall Rules on page 744.

4 Use the **VPN Crypto Map** drop-down menu to select or override the Crypto Map configuration applied to this virtual interface.

The VPN Crypto Map entry defines the type of VPN connection and its parameters. For more information see Defining Profile VPN Settings on page 217.

5 Click **OK** to save the changes and overrides to the Security screen.

Click **Reset** to revert to the last saved configuration.

### Dynamic Routing Configuration

To configure the VLAN Dynamic Routing configuration:

1 Select the **Dynamic Routing** tab.

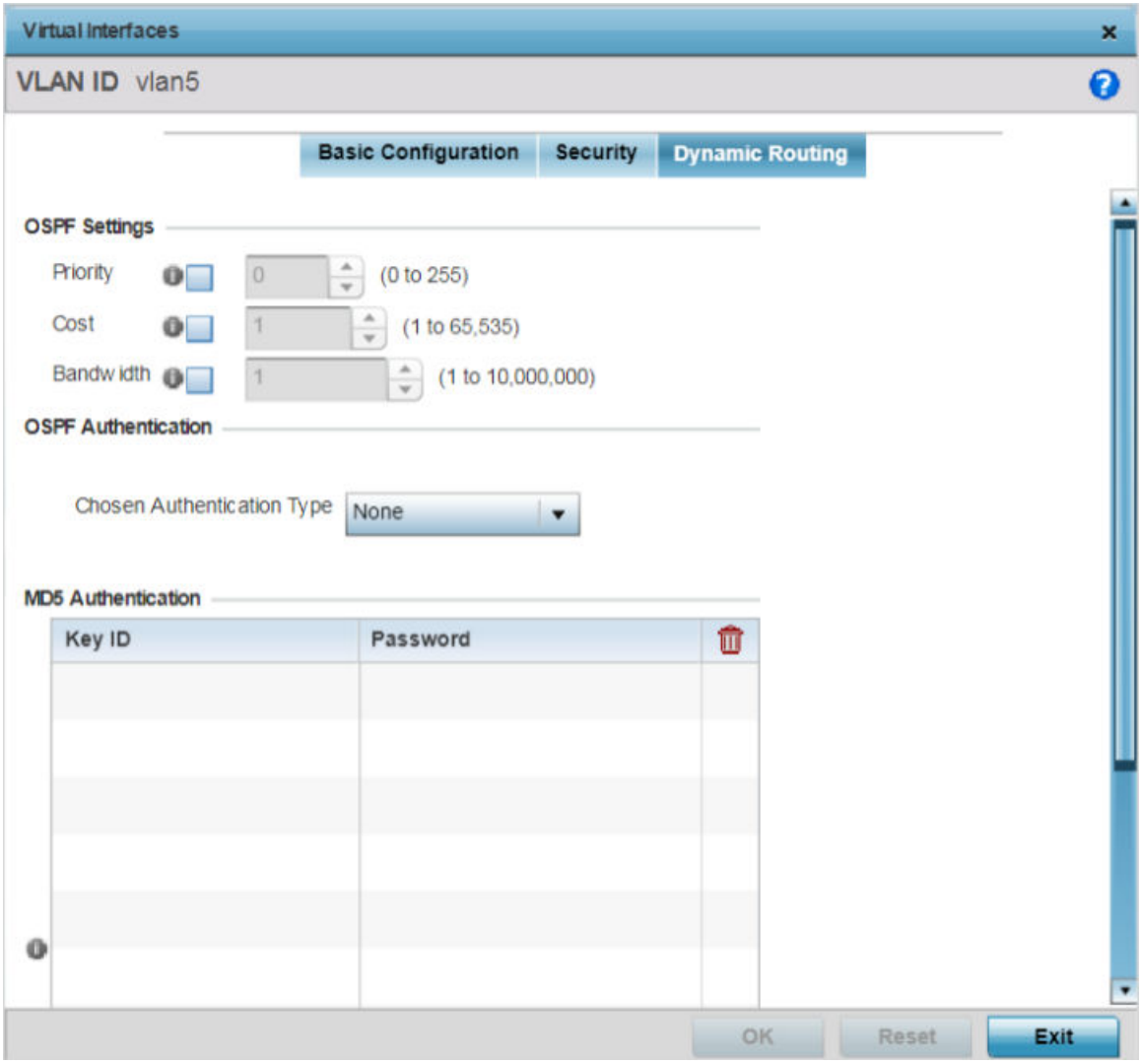



**Figure 38: Profile Overrides - Virtual Interfaces Dynamic Routing Screen**

2 Define or override the following parameters in the OSPF Settings field:

| | |
|---|---|
| Priority | Select this option to enable or disable OSPF priority settings. Use the spinner to configure a value from 0 - 255. This option sets the priority of this interface becoming the DR *(Designated Router)* for the network. DRs provide routing updates to the network by maintaining a complete topology table of the network and sends the updates to the other routers in the network using multicast. Setting a high value increases the chance of this interface becoming a DR. Setting this value to zero prevents this interface from being elected a DR. |
| Cost | Select this option to enable or disable OSPF cost settings. Use the spinner to configure a cost value from 1 - 65535. Use this option to set the OSPF cost of this interface. OSPF cost is the overhead required to send a packet over this interface. |
| Bandwidth | Set the OSPF bandwidth from 1 - 10,000,000 KBps. |

3 Configure the **OSPF Authentication Type** settings by selecting from the drop-down list.

The available options are **`None`**, **`null`**, **`simple-password`**, and **`message-digest`**.

4 Select **+ Add Row** at the bottom of the MD5 Authentication table to add the Key ID and Password used for an MD5 validation of authenticator credentials.

| | |
|---|---|
| Key ID | Use the spinner control to set the unique OSPF message digest authentication key ID. The available range is from 1 - 255. The password is the OSPF key either displayed as series or asterisks or in plain text (by selecting **Show**). |
| Password | Set the OSPF password. This value is displayed as “asterisk” (*). Select **Show** to expose the characters in the password. |

5 Click **OK** to save the changes and overrides to the Security screen.

Click **Reset** to revert to the last saved configuration.

### *Port Channel Configuration*

Controller, service platform and access point profiles can be applied customized port channel settings as part of their interface configuration.

Note

WiNG 7.1 release does not support Port Channel configuration on AP505i and AP510i model access points.

To define a port channel configuration for a device profile:

1 Select **Configuration → Devices → System Profile** from the web UI.

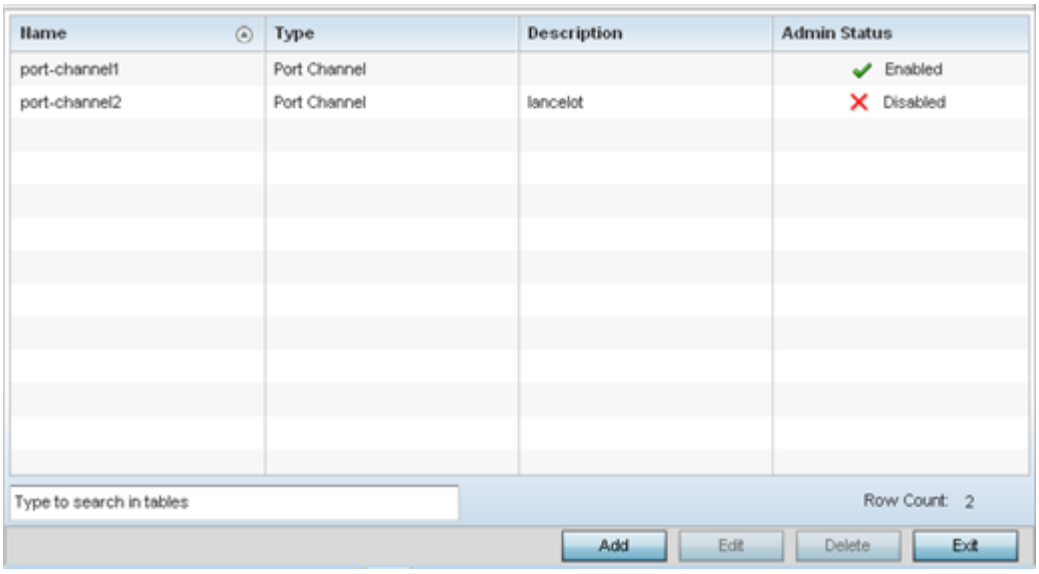
A list of device profiles is displayed in the right-hand UI. This list contains default and user-defined profiles.

2 Select a profile from those listed on the screen.

The profile's configuration menu is displayed.

3 Expand the **Interface** menu and select **Port Channels**.

The Port Channels screen displays.




4 Refer to the following to review existing port channel configurations and their current status:

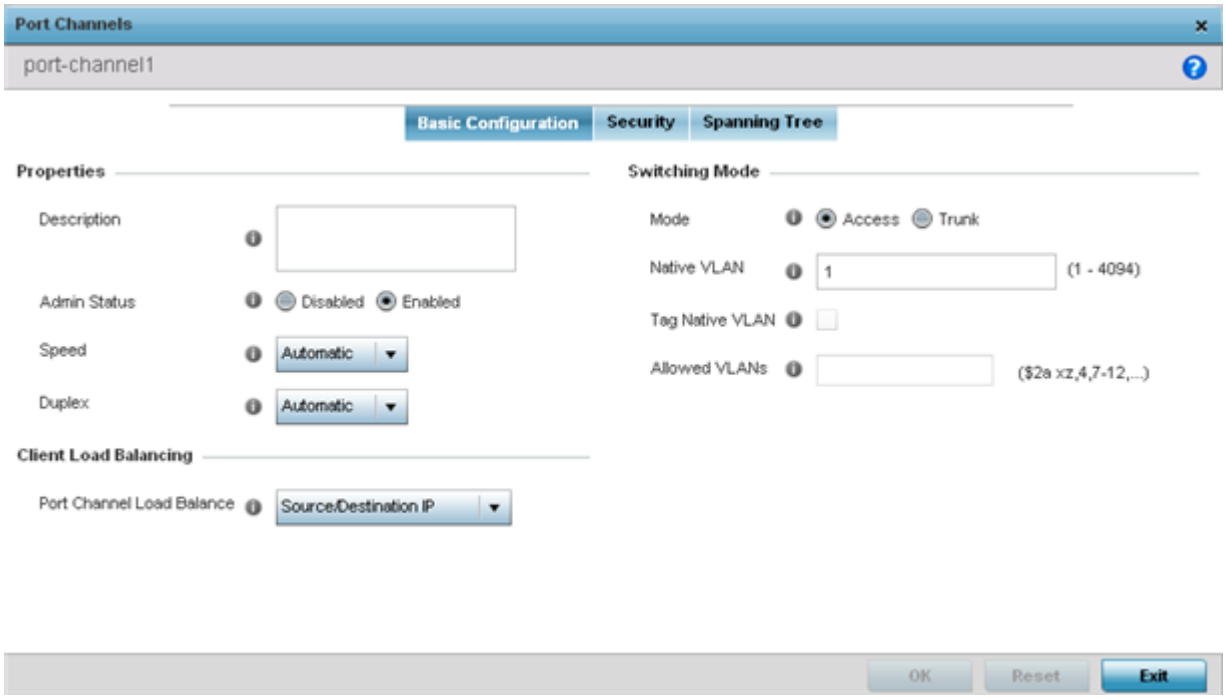
| | |
|---|---|
| Name | Displays the port channel's numerical identifier assigned to it when it was created. The numerical name cannot be modified as part of the edit process. |
| Type | Displays whether the type is port channel. |
| Description | Lists a short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations. |
| Admin Status | A green checkmark defines the listed port channel as active and currently enabled with the profile. A red "X" defines the port channel as currently disabled and not available for use. The interface status can be modified with the port channel configuration as required. |

### Port Channel Basic Configuration

You can add a new port channel configuration or edit an existing configuration.

1 Select **Add** to create a new manual session, **Edit** to modify an existing configuration. To remove a selected port channel configuration select **Delete**.

The port channel Basic Configuration screen displays by default.




2 Set the following port channel **Properties**:

| | |
|---|---|
| Description | Enter a brief description for the port channel (64 characters maximum). The description should reflect the port channel's intended function. |
| Admin Status | Select the *Enabled* radio button to define this port channel as active to the profile it supports. Select the *Disabled* radio button to disable this port channel configuration within the profile. It can be activated at any future time when needed. The default setting is enabled. |
| Speed | Select the speed at which the port channel can receive and transmit the data. Select either *10 Mbps*, *100 Mbps*, *1000 Mbps*. Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Automatic is selected. Select *Automatic* to enable the port channel to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting. |
| Duplex | Select either *Half*, *Full* or *Automatic* as the duplex option. Select Half duplex to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted. Like a Full duplex transmission, a Half duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port channel at the same time. Using Full duplex, the port channel can send data while receiving data as well. Select Automatic to dynamically duplex as port channel performance needs dictate. Automatic is the default setting. |

3 Use the **Port Channel Load Balance** drop-down menu to define whether port channel load balancing is conducted using a Source/Destination IP or a Source/Destination MAC. Source/Destination IP is the default setting.

4 Define the following **Switching Mode** parameters to apply to the port channel configuration:

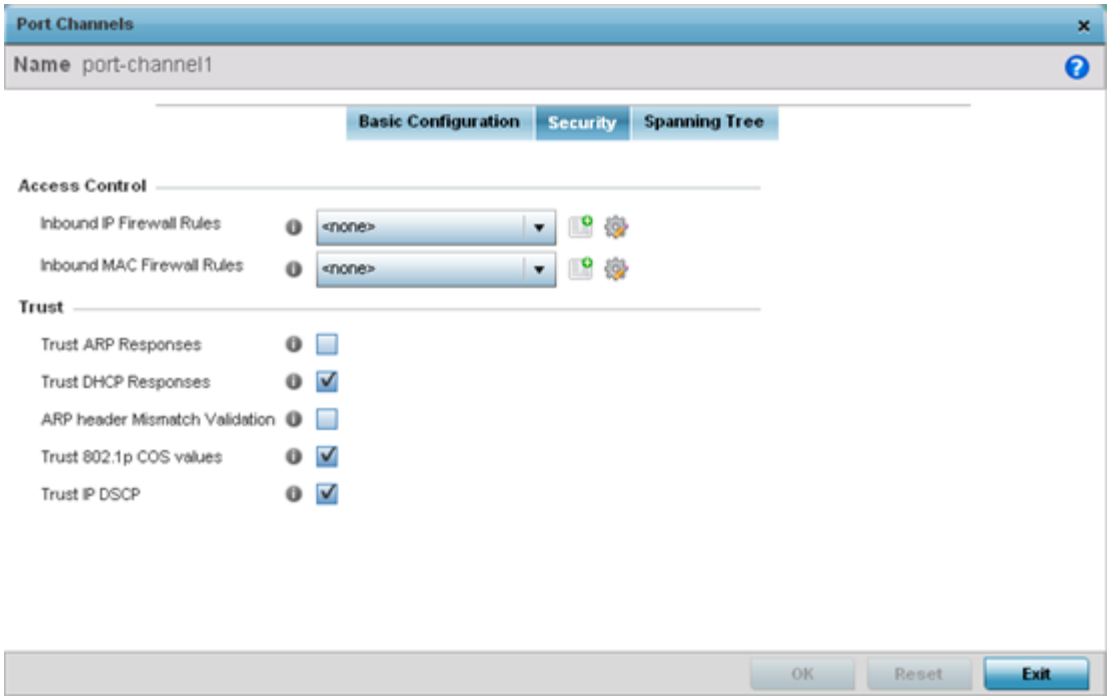
| | |
|---|---|
| Mode | Select either the *Access*or *Trunk* radio button to set the VLAN switching mode over the port channel. If Access is selected, the port channel accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default setting. |
| Native VLAN | Use the spinner control to define a numerical ID between 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using trunk mode. The default value is 1. |
| Tag the Native VLAN | Select the checkbox to tag the native VLAN. WiNG managed devices support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default. |
| Allowed VLANs | Selecting *Trunk* as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the port channel. |

5 Select **OK** to save the changes made to the port channel Basic Configuration. Select **Reset** to revert to the last saved configuration.

### Port Channel Security

To define a port channel's security configuration.

1 Select the **Security** tab.




2 Refer to the Access Control section. As part of the port channel's security configuration, Inbound IP and MAC address firewall rules are required.

Use the Inbound IP Firewall Rules and MAC Inbound Firewall Rules drop-down menus to select firewall rules to apply to this profile's port channel configuration.

The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

If a firewall rule does not exist suiting the data protection needs of the target port channel configuration, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing firewall rule configuration. For more information, see Wireless Firewall on page 730.

3 Refer to the Trust field to define the following:

| | |
|---|---|
| Trust ARP Responses | Select the check box to enable ARP trust on this port channel. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled. |
| Trust DHCP Responses | Select the check box to enable DHCP trust. If enabled, only DHCP responses are trusted and forwarded on this port channel, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled. |
| ARP header Mismatch Validation | Select the check box to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled. |
| Trust 802.1p COS values | Select the check box to enable 802.1p COS values on this port channel. The default value is enabled. |
| Trust IP DSCP | Select the check box to enable IP DSCP values on this port channel. The default value is enabled. |

4 Set the following IPv6 Settings:

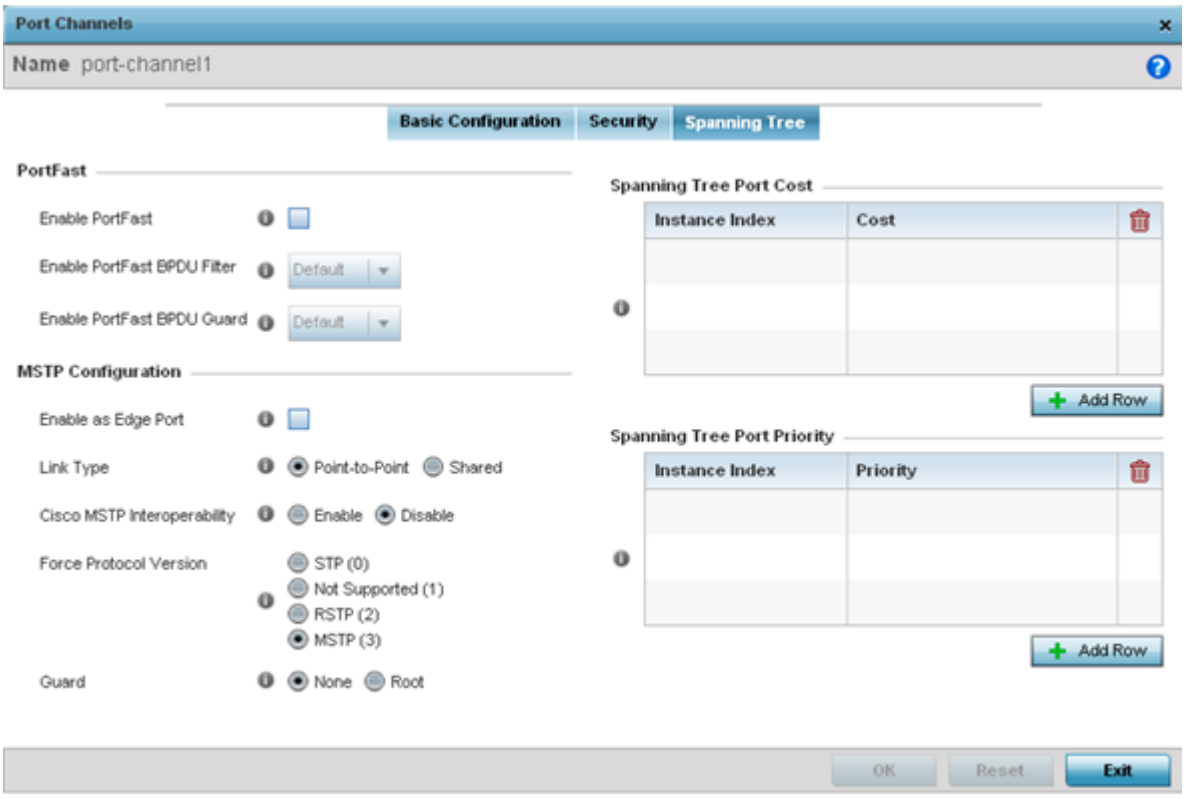
| | |
|---|---|
| Trust ND Requests | Select to enable the trust of neighbor discovery requests required on an IPv6 network. This setting is disabled by default. |
| Trust DHCPv6 Responses | Select to enable the trust all DHCPv6 responses. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network. This setting is enabled by default. |
| ND Header Mismatch Validation | Select to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This option is disabled by default. |
| RA Guard | Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This option is disabled by default. |

5 Select **OK** to save the changes to the security configuration. Select **Reset** to revert to the last saved configuration.

### Port Channel Spanning Tree

To define a port channel' spanning tree configuration:

1 Select the **Spanning Tree** tab.




2 Define the following PortFast parameters for the port channel's MSTP configuration:

| | |
|---|---|
| Enable PortFast | Select the check box to enable drop-down menus for both the port Enable Portfast BPDU Filter and Enable Portfast BPDU guard options. This setting is disabled by default. |
| PortFast BPDU Filter | Select *Enable* to invoke a BPDU filter for this portfast enabled port channel. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. The default setting is None. |
| PortFast BPDU Guard | Select *Enable* to invoke a BPDU guard for this portfast enabled port channel. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. The default setting is None. |

3 Set the following MSTP Configuration parameters for the port channel:

| | |
|---|---|
| Enable as Edge Port | Select the check box to define this port as an edge port. Using an edge (private) port, you can isolate devices to prevent connectivity over this port channel. This setting is disabled by default. |
| Link Type | Select either the *Point-to-Point* or *Shared* radio button. Selecting Point-to-Point indicates the port should be treated as connected to a point-to-point link. Selecting Shared indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while the one connected to the wireless device is a point-to-point link. Point-to-Point is the default setting. |
| Cisco MSTP Interoperability | Select either the *Enable* or *Disable* radio buttons. This enables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default. |
| Force Protocol Version | Sets the protocol version to either *STP(0)*, *Not Supported(1)*, *RSTP(2)* or *MSTP(3)*. MSTP is the default setting. |
| Guard | Determines whether the port channel enforces root bridge placement. Setting the guard to *Root* ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the *bridge receives superior* (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position. |

4 Refer to the Spanning Tree Port Cost table. Select **+ AddRow** as needed to include additional indexes.

Define an Instance Index using the spinner control and then set the Cost. The default path cost depends on the user defined port speed. The cost helps determine the role of the port channel in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

| Speed | Default Path Cost |
|---|---|
| <=100000 bits/sec | 200000000 |
| <=1000000 bits/sec | 20000000 |
| <=10000000 bits/sec | 2000000 |
| <=100000000 bits/sec | 200000 |
| <=1000000000 bits/sec | 20000 |
| <=10000000000 bits/sec | 2000 |
| <=100000000000 bits/sec | 200 |

| Speed | Default Path Cost |
|---|---|
| <=1000000000000 bits/sec | 20 |
| >1000000000000 bits/sec | 2 |

5

6 Refer to the Spanning Tree Port Priority table. Select **+ Add Row** needed to include additional indexes.

Define an Instance Index using the spinner control and then set the Priority. The lower the priority, a greater likelihood of the port becoming a designated port.

7 Select **OK** to save the changes made to the Ethernet Port Spanning Tree configuration. Select **Reset** to revert to the last saved configuration.

### *Access Point Radio Configuration*

Access points can have their radio configurations modified by their management controller, service platform or peer access point. Take care not to modify an access point's configuration using its resident Web UI, CLI or SNMP interfaces when managed by a profile, or risk the access point having a configuration independent from the profile until the profile can be uploaded to the access point again from its managing device.

To define an access point radio configuration from an associated peer access point controller AP, controller or NX service platform:

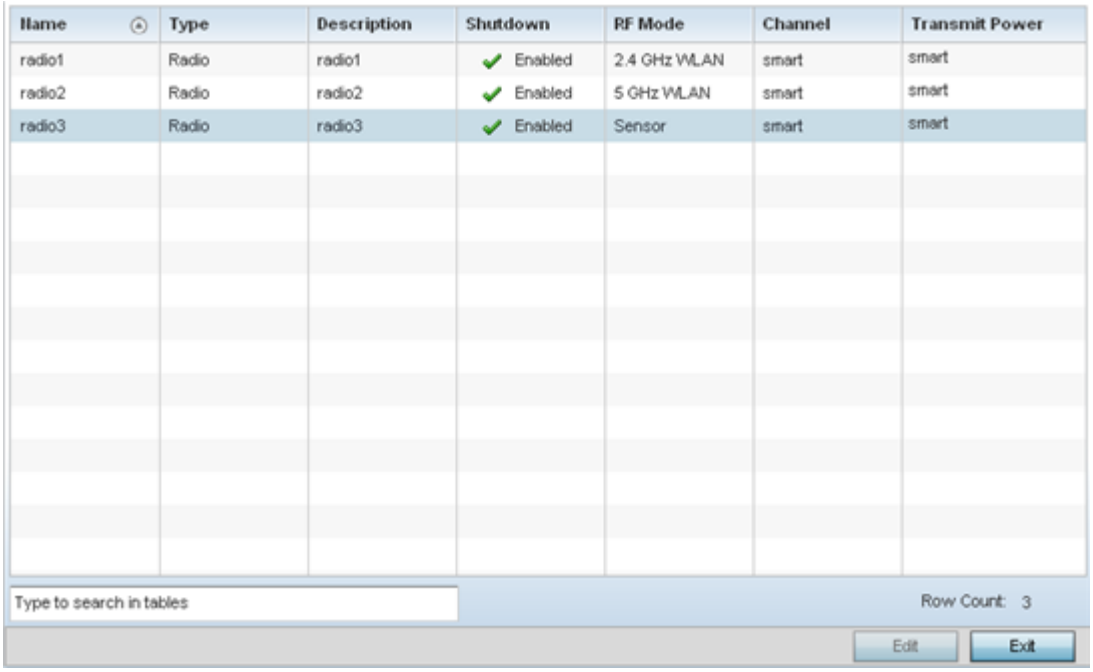
1 Select **Configuration → Devices → System Profile** from the web UI.

A list of device profiles is displayed in the right-hand UI. This list contains default and user-defined profiles.

2 Select a profile from those listed on the screen.

The profile's configuration menu is displayed.

3 Expand the **Interface** menu and select **Radios**.




4 Review the following to determine whether a radio configuration requires modification to better support the managed network:

| | |
|---|---|
| Name | Displays whether the reporting radio is the access point's radio1, radio2 or radio3. |
| Type | Displays the type of radio housed by each listed access point. |
| Description | Displays a brief description of the radio provided by the administrator when the radio's configuration was added or modified. |
| Admin Status | A green checkmark defines the listed radio as active and enabled with its supported profile. A red "X" defines the radio as currently disabled. |
| RF Mode | Displays whether each listed radio is operating in the 802.11a/n or 802.11b/g/n radio band. If the radio is a dedicated sensor, it will be listed as a sensor to define the radio as not providing typical WLAN support. If the radio is a client-bridge, it provides a typical bridging function and does not provide WLAN support. The radio band is set from within the Radio Settings tab. |
| Channel | Lists the channel setting for the radio. Smart is the default setting. If set to smart, the access point scans non-overlapping channels listening for beacons from other access points. After the channels are scanned, it selects the channel with the fewest access points. In the case of multiple access points on the same channel, it selects the channel with the lowest average power level. |
| Transmit Power | Lists the transmit power for each radio displayed as a value in milliwatts. |

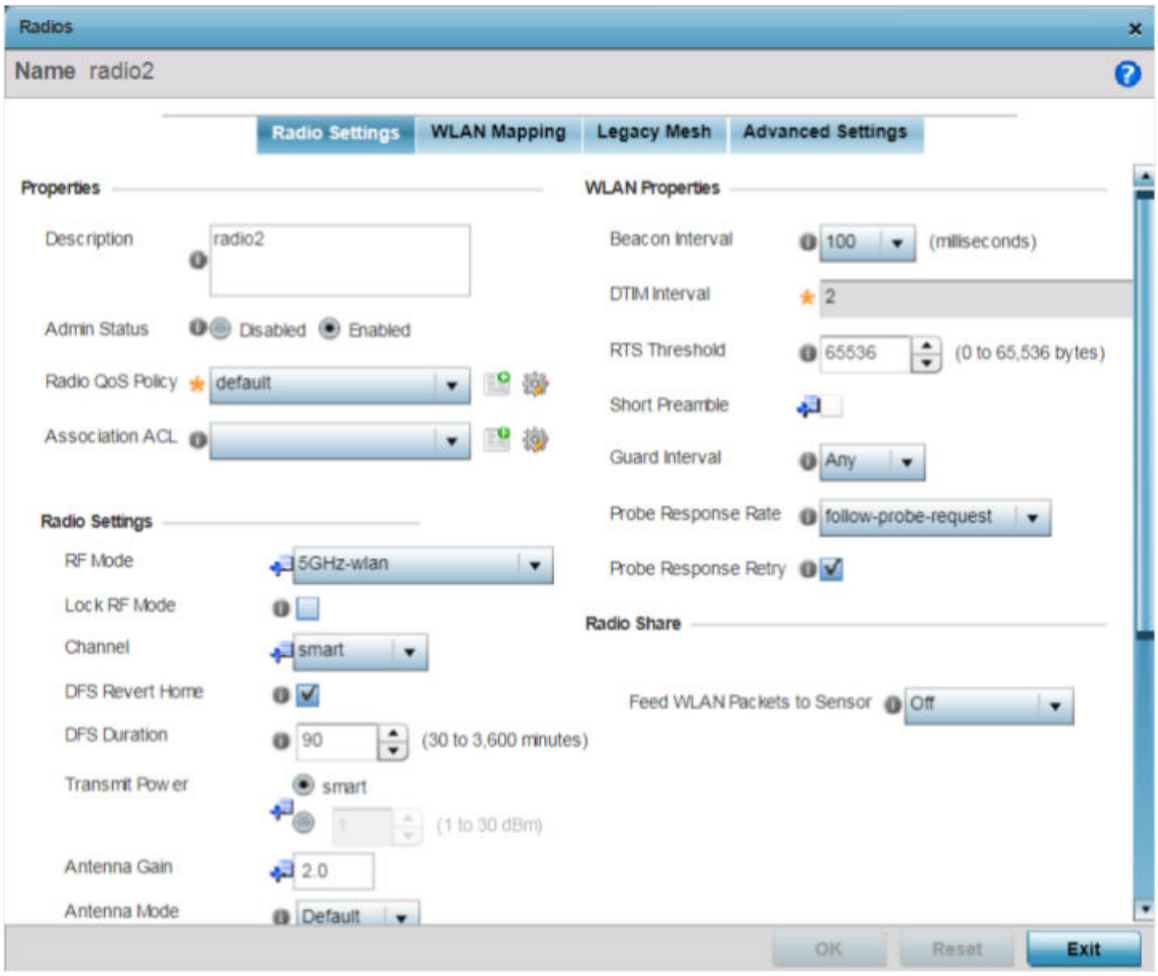
5 If required, select a radio configuration and select the **Edit** button to modify its configuration.

### Radio Settings

Use the Radio Settings screen to apply QoS, ACL, operational mode, WLAN attributes and sensor configuration settings to the radio.

To edit an access point's radio settings:

1 Select the radio and select the **Edit**.




The Radio Settings tab displays by default.

2 Define the following radio configuration parameters from within the Properties field:

| | |
|---|---|
| Description | Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations. |
| Admin Status | Select the *Enabled* radio button to define this radio as active to the profile it supports. Select the *Disabled* radio button to disable this radio configuration within the profile. It can be activated at any future time when needed. The default setting is enabled. |

| | |
|---|---|
| Radio QoS Policy | Use the drop-down menu to specify an existing QoS policy to apply to the access point radio in respect to its intended radio traffic. If there's no existing suiting the radio's intended operation, select the *Create* icon to define a new QoS policy that can be applied to this profile. |
| Association ACL | Use the drop-down menu to specify an existing Association ACL policy to apply to the access point radio. An Association ACL is a policy-based ACL that either prevents or allows wireless clients from connecting to an access point radio. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, its compared against applied ACLs to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped. Select the *Create* icon to define a new Association ACL that can be applied to this profile. |

3 Set the following profile **Radio Settings** for the selected access point radio:

| | |
|---|---|
| RF Mode | The radio can be configured to provide WLAN service for 2.4 GHz and 5 GHz enabled clients. You can also set the radio to provide sensor support, scan-ahead support, or function as a client bridge.<br>Set the mode to either *2.4 GHz WLAN* or *5 GHz WLAN* depending on the radio's intended client support requirement.<br>Set the mode to *Sensor* if using the radio for rogue device detection. To set a radio as a detector, disable Sensor support on the other access point radio.<br>Set the mode to *scan-ahead* in DFS aware countries to allow a mesh points secondary radio to scan for an alternative channel for backhaul transmission in the event of a radar event on the principal radio. The secondary radio is continually monitoring the alternate channel, which means the principal radio can switch channels and transmit data immediately without waiting for the channel availability check.<br>Set the mode to *bridge* to configure the radio as a client bridge. A client bridge enables the access point to connect to a third party access point and bridge frames to it.<br>The client-bridge is supported only on the following access point models: AP6522, AP6562, AP7522, AP7532, AP7602, AP7612, AP7622, AP7632 and AP7622<br><br>**Note:** For AP510 model access point, you can provide 5 GHz WLAN support on both radio 1 and radio 2.<br><br>**Note:** The *scan-ahead* and *bridge* RF modes are not supported on the AP 505i and AP510i model access points.<br><br>**Note:** For information on the possible modes of operations for AP505 and AP510 radios, see ap510i and ap505i. |
| Lock RF Mode | Select the check box to lock Smart RF for this radio. The default setting is disabled. |
| DFS Revert Home | Select this option to revert to the home channel after a DFS evacuation period. |

| | |
|---|---|
| Channel | Use the drop-down menu to select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select Smart for the radio to scan non-overlapping channels listening for beacons from other access points. After channels are scanned, the radio selects the channel with the fewest access points. In the case of multiple access points on the same channel, it selects the channel with the lowest average power level. The default value is Smart. Channels with a “w” appended to them are unique to the 40 MHz band. Channels with a “ww” appended to them are 802.11ac specific, and are unique to the 80 MHz band. |
| Transmit Power | Set the transmit power of the selected access point radio. If using a dual or three radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value. |
| Antenna Gain | Set the antenna between 0.00 - 15.00 dBm. The access point's Power *Management Antenna Configuration File* (PMACF) automatically configures the access point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00. |
| Antenna Mode | Set the number of transmit and receive antennas on the access point. 1x1 is used for transmissions over just the single "A" antenna, 1x3 is used for transmissions over the "A" antenna and all three antennas for receiving. 2x2 is used for transmissions and receipts over two antennas for dual antenna models. 3x3x3 is used for transmissions and receipts over three antennas models.The default setting is dynamic based on the access point model deployed and its transmit power settings. |
| Enable Antenna Diversity | Select this box to enable antenna diversity on supported antennas. Antenna diversity uses two or more antennas to increase signal quality and strength. This option is disabled by default. |
| Wireless Client Power | Select this option to specify the transmit power on supported wireless clients. If this is enabled set a client power level between 0 to 20 dBm. This option is disabled by default. |
| Dynamic Chain Selection | Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default. |

| | |
|---|---|
| Data Rates | Once the radio band is provided, the Data Rates drop-down menu populates with rate options depending on the 2.4 or 5 GHz band selected. If the radio band is set to Sensor or Detector, the Data Rates drop-down menu is not enabled, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together. When using 802.11n (in either the 2.4 or 5 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).<br>If dedicating the radio to either 2.4 or 5 Ghz support, a Custom Rates option is available to set a *modulation and coding scheme* (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). If Basic is selected within the 802.11n Rates field, the MCS0-7 option is auto selected as a Supported rate and that option is greyed out. If Basic is not selected, any combination of MCS0-7, MCS8-15 and MCS16-23 can be supported, including a case where MCS0-7 and MCS16-23 are selected and not MCS8-15. The MCS0-7 and MCS8-15 options are available to each support access point. However, the MCS16-23 option is only available to AP 8132 model access points and its ability to provide 3x3x3 MIMO support.<br>Refer to the bottom of this page for 802.11an and 802.11ac MCS dates rates in detail, both with and without *short guard intervals* (SGI).<br><br>**Note:** For information on supported data rates see, SUPPORTED DATA RATES |
| Radio Placement | Use the drop-down menu to specify whether the radio is located *Indoors* or *Outdoors*. The placement should depend on the country of operation and its regulatory domain requirements for radio emissions. The default setting is Indoors. |
| Max Clients | Use the spinner control to set a maximum permissible number of clients to connect with this radio. The available range is between 0 - 256 clients. The default value is 256.<br><br>**Note:** The AP505 and AP510 support a maximum of 250 clients per radio. |
| Rate Selection Method | Specify a radio selection method for the radio. The selection methods are: *Standard*: standard monotonic radio selection method will be used. *Opportunistic*: sets opportunistic radio link adaptation as the radio selection method. This mode uses opportunistic data rate selection to provide the best throughput. |

4 Set the following profile **WLAN Properties** for the selected access point radio.

| | |
|---|---|
| Beacon Interval | Set the interval between radio beacons in milliseconds (either 50, 100 or 200). A beacon is a packet broadcast by adopted radios to keep the network synchronized. The beacon includes the WLAN service area, radio address, broadcast destination addresses, time stamp and indicators about traffic and delivery such as a DTIM. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default value is 100 milliseconds. |
| DTIM Interval BSSID | Set a DTIM Interval to specify a period for DTIM *(Delivery Traffic Indication Messages)*. A DTIM is periodically included in a beacon frame transmitted from adopted radios. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates broadcast and multicast frames (buffered at the access point) are soon to arrive. These are simple data frames that require no acknowledgment, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive. |
| RTS Threshold | Specify a RTS *(Request To Send)* threshold (between 1 - 2,347 bytes) for use by the WLAN's adopted access point radios. RTS is a transmitting station's signal that requests a CTS *(Clear To Send)* response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.<br>Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.<br>Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.<br>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold. |
| Short Preamble | If using an 802.11bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink/Polycomm phones) require long preambles. The default value is disabled. |

| | |
|---|---|
| Guard Interval | Use the drop-down menu to specify a *Long* or *Any* guard interval. The guard interval is the space between the packets being transmitted. The guard interval is there to eliminate ISI *(inter-symbol interference)*. ISI occurs when echoes or reflections from one transmission interfere with another. Adding time between transmissions allows echo's and reflections to settle before the next packet is transmitted. A shorter guard interval results in a shorter times which reduces overhead and increases data rates by up to 10%.The default value is Long. |
| Probe Response Rate | Use the drop-down menu to specify the data transmission rate used for the transmission of probe responses. Options include, *highest-basic*, *lowest-basic* and *follow-probe-request* (default setting). |
| Probe Response Retry | Select the check box to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled. |

5 Select a mode from the **Feed WLAN Packets to Sensor** check box in the Radio Share section to enable this feature.

Select either *Inline* or *Promiscuous* mode to allow the packets the radio is switching to also be used by the WIPS analysis module. This feature can be enabled in two modes: an inline mode where the wips sensor receives the packets from the radios with radio operating in normal mode. A promiscuous mode where the radio is configured to a mode where it receives all packets on the channel whether the destination address is the radio or not, and the wips module can analyze them.

*SUPPORTED DATA RATES*

802.11n MCS rates are defined as follows for MCS 1-3 streams, both with and without SGI:

| *MCS-1Stream Index* | Number of Streams | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI |
|---|---|---|---|---|---|
| 0 | 1 | 6.5 | 7.2 | 13.5 | 15 |
| 1 | 1 | 13 | 14.4 | 27 | 30 |
| 2 | 1 | 19.5 | 21.7 | 40.5 | 45 |
| 3 | 1 | 26 | 28.9 | 54 | 60 |
| 4 | 1 | 39 | 43.4 | 81 | 90 |
| 5 | 1 | 52 | 57.8 | 108 | 120 |
| 6 | 1 | 58.5 | 65 | 121.5 | 135 |
| 7 | 1 | 65 | 72.2 | 135 | 150 |

| *MCS-2Stream Index* | Number of Streams | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI |
|---|---|---|---|---|---|
| 0 | 2 | 13 | 14.4 | 27 | 30 |
| 1 | 2 | 26 | 28.9 | 54 | 60 |
| 2 | 2 | 39 | 43.4 | 81 | 90 |
| 3 | 2 | 52 | 57.8 | 108 | 120 |
| 4 | 2 | 78 | 86.7 | 162 | 180 |
| 5 | 2 | 104 | 115.6 | 216 | 240 |

| *MCS-2Stream Index* | Number of Streams | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI |
|---|---|---|---|---|---|
| 6 | 2 | 117 | 130 | 243 | 270 |
| 7 | 2 | 130 | 144.4 | 270 | 300 |

| *MCS-3Stream Index* | Number of Streams | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI |
|---|---|---|---|---|---|
| 0 | 3 | 19.5 | 21.7 | 40.5 | 45 |
| 1 | 3 | 39 | 43.3 | 81 | 90 |
| 2 | 3 | 58.5 | 65 | 121.5 | 135 |
| 3 | 3 | 78 | 86.7 | 162 | 180 |
| 4 | 3 | 117 | 130.7 | 243 | 270 |
| 5 | 3 | 156 | 173.3 | 324 | 360 |
| 6 | 3 | 175.5 | 195 | 364.5 | 405 |
| 7 | 3 | 195 | 216.7 | 405 | 450 |

802.11ac MCS rates (theoretical throughput for single spatial streams) are defined as follows, both with and without SGI:

| *MCS Index* | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI | 80 MHz No SGI | 80 MHz With SGI |
|---|---|---|---|---|---|---|
| 0 | 6.5 | 7.2 | 13.5 | 15 | 29.3 | 32.5 |
| 1 | 13 | 14.4 | 27 | 30 | 58.5 | 65 |
| 2 | 19.5 | 21.7 | 40.5 | 45 | 87.8 | 97.5 |
| 3 | 26 | 28.9 | 54 | 60 | 117 | 130 |
| 4 | 39 | 43.3 | 81 | 90 | 175.5 | 195 |
| 5 | 52 | 57.8 | 108 | 120 | 234 | 260 |
| 6 | 58.5 | 65 | 121.5 | 135 | 263.3 | 292.5 |
| 7 | 65 | 72.2 | 135 | 150 | 292.5 | 325 |
| 8 | 78 | 86.7 | 162 | 180 | 351 | 390 |
| 9 | N/A | N/A | 180 | 200 | 390 | 433.3 |

6 Select **OK** to save the changes made within the screen. Select **Reset** to revert to the last saved configuration.

**Table 3: AP510 Radio 1 and Radio 2: Possible Modes of Operation**

| | | |
|---|---|---|
| **`Option 1`** | *Radio 1:* | Set to 2.4 GHz WLAN, Channels 1 - 11 in the 20 MHz /40 MHz bandwidths |
| | *Radio 2:* | Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths |

**Table 3: AP510 Radio 1 and Radio 2: Possible Modes of Operation (continued)**

| | | |
|---|---|---|
| **Option 2** | *Radio 1:* | Set to Sensor |
| | *Radio 2:* | Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths |
| **Option 3** | *Radio 1:* | Set to 5 GHz, Channels 36 - 64 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths |
| | *Radio 2:* | Set to 5 GHz, Channels 100 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths |

**Table 4: AP505i Radio 1 and Radio 2: Possible Modes of Operation**

| | | |
|---|---|---|
| **Option 1** | *Radio 1:* | Set to 2.4 GHz WLAN, Channels 1 - 11 in the 20 MHz /40 MHz bandwidths |
| | *Radio 2:* | Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz |
| **Option 2** | *Radio 1:* | Set to Sensor. |
| | *Radio 2:* | Set to Sensor. |

### WLAN Mapping / Mesh Mapping

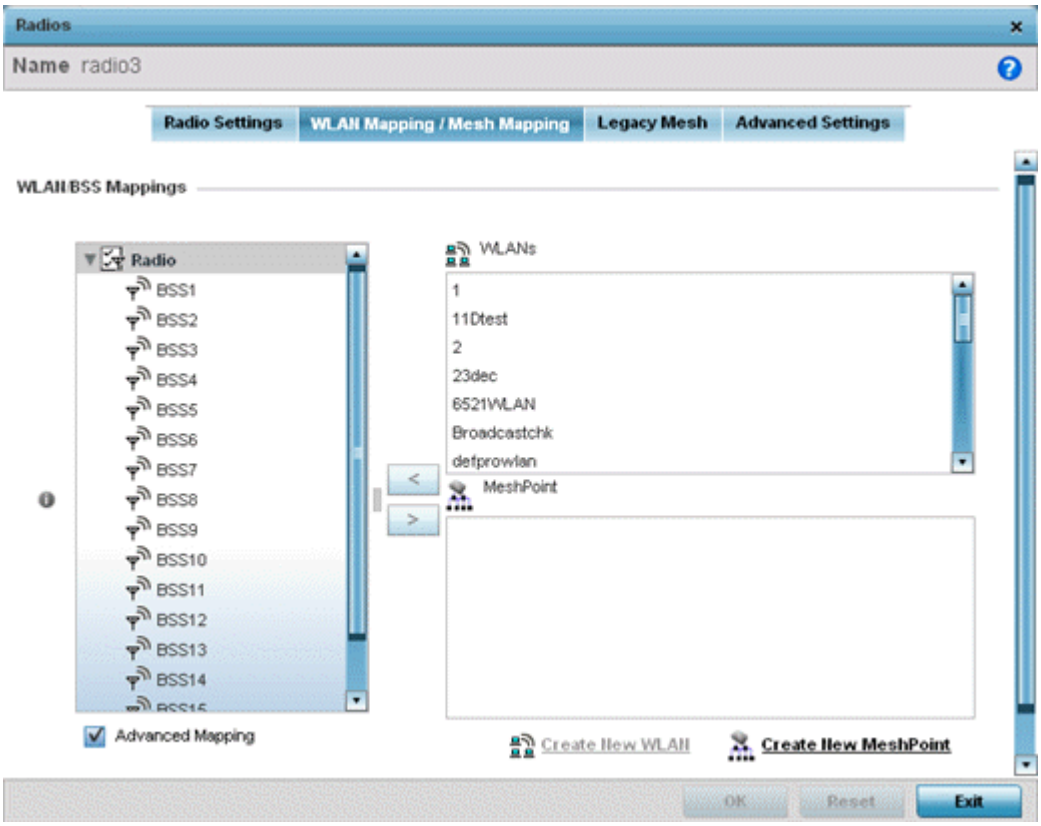
You can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If you are using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Note

WiNG 7.1 release does not support MeshConnex on AP505i and AP510i model access points. This feature will be supported in future releases.

To set a radio's WLAN mapping configuration:

1 Select the **WLAN Mapping** tab.




2 Refer to the WLAN/BSS Mappings field to set WLAN BSSID assignments for an existing access point deployment.

Use the '**<**' or '**>**' buttons to assign WLANs and mesh points to the available BSSIDs.

You can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio. Each supported access point model can support up to 8 BSS IDs.

3 Select **Advanced Mapping** to enable WLAN mapping to a specific BSS ID.

4 Select **OK** to save the changes to the WLAN Mapping. Select **Reset** to revert to the last saved configuration.

### Mesh Legacy

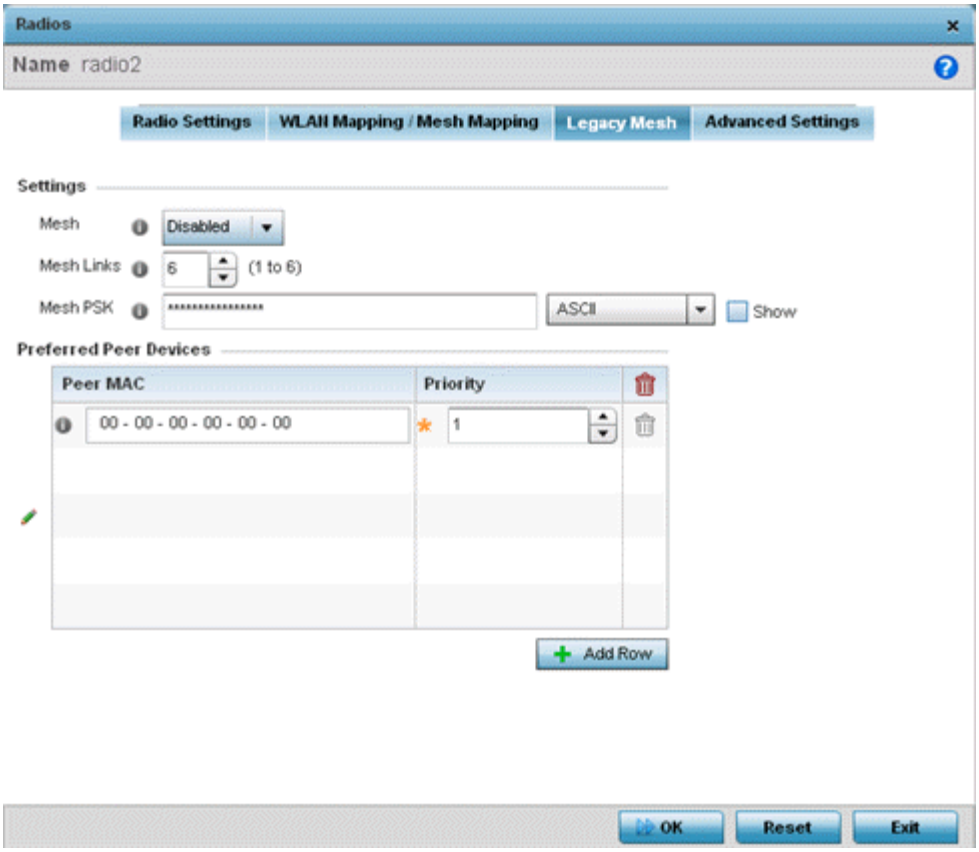
Each radio can have a unique mesh mode and link configuration. This provides a customizable set of connections to other mesh supported radios within the same radio coverage area.

Note

WiNG 7.1 release does not support MeshConnex on AP505i and AP510i model access points. This feature will be suported in future releases.

To set/override a radio's legacy mesh configuration:

1 Select the **Legacy Mesh** tab.




2 Refer to the Advanced Settings field to define basic mesh settings for the access point radio.

| | |
|---|---|
| Mesh | Use the drop-down menu to set the mesh mode for this radio. Available options are *Disabled*, *Portal* or *Client*. Setting the mesh mode to Disabled deactivates all mesh activity on this radio. Setting the mesh mode to Portal turns the radio into a mesh portal. This will start the radio beaconing immediately and accept connections from other mesh nodes. Setting the mesh mode to client enables the radio to operate as a mesh client and scan and connect to mesh portals or nodes connected to portals. |
| Mesh Links | Specify the number of mesh links allowed by the radio. The radio can have between 1-6 mesh links when the radio is configured as a Portal or Client. |
| Mesh PSK | Provide the encryption key in either ASCII or Hex format. Administrators must ensure this key is configured on the access point when staged for mesh, added to the mesh client and to the portal access point's configuration on the controller or service platform. Select Show to expose the characters used in the PSK.<br><br>Note: Only single hop mesh links are supported at this time.<br><br>Note: The mesh encryption key is configurable from the CLI using the command 'mesh → psk'. Administrators must ensure this key is configured on the AP when it is being staged for mesh, and also added to the mesh client as well as to the portal APs configuration on the controller. |

3 Refer to the Preferred Peer Device table to add mesh peers. For each peer added, enter its MAC Address and a Priority between 1 and 6. The lower the priority number the higher priority it'll be given when connecting to mesh infrastructure.

4 Select the **+ Add Row** and define the following MAC addresses to preferred mesh connection mappings:

| | |
|---|---|
| Priority | Use this spinner control to set a priority (1 -6) for connection preference. |
| Peer MAC | For each priority value, define the MAC address of the associated peer device. Use this option to are define MAC addresses representing peer devices for the radio to connect to in mesh mode. |

5 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

### Client Bridge Settings

An access point's radio can be configured to form a bridge between its wireless/wired clients and an infrastructure WLAN. The bridge radio authenticates and associates with an infrastructure WLAN access point. After successful association, the access point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, thereby providing the clients access to the infrastructure WLAN resources.

The client-bridge is supported only on the following access point models: AP6522, AP6562, AP7522, AP7532, AP7602, AP7612, AP7622, AP7632 and AP7622.

Note

WiNG 7.1 release does not support Client Bridge configuration on AP505i and AP510i model access points. This feature will be supported in future releases.

To configure a radio's client bridge settings:

1 Select the **Client Bridge Settings** tab.

The selected radio's client bridge configuration screen displays.

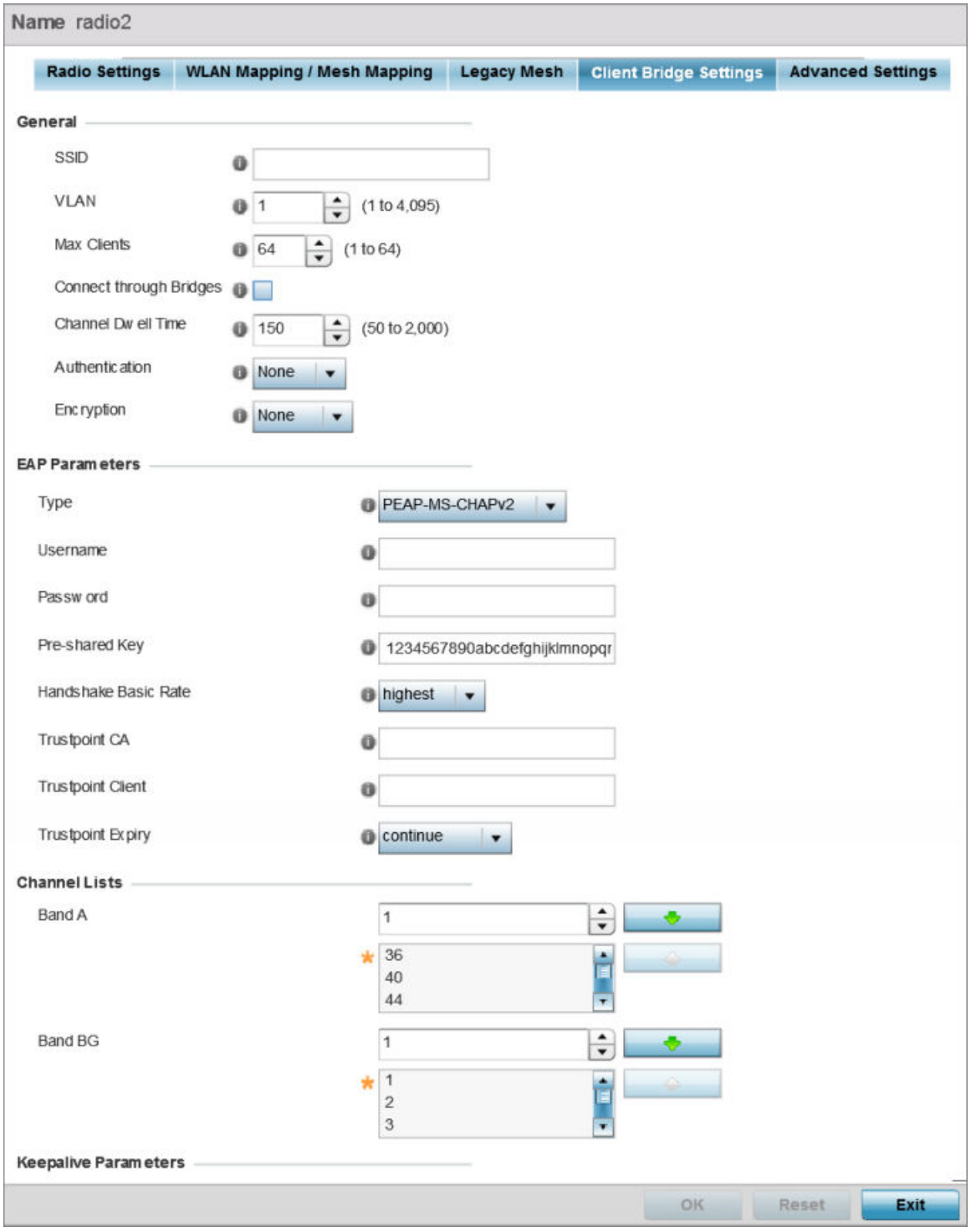



**Figure 39: Radio Interface - Client Bridge Configuration Screen**

2 Define the following General settings:

| | |
|---|---|
| SSID | Set the infrastructure WLAN's SSID, with which the client-bridge access point associates. |
| VLAN | Set the VLAN to which the bridged clients' sessions are mapped after successful association with the infrastructure WLAN. Once mapped, the client bridge communicates with permitted hosts over the infrastructure WLAN. Specify the VLAN from 1 to 4095. |
| Max Clients | Set the maximum number of client-bridge access points that can associate with the infrastructure WLAN. Specify a value from 1 to 64. The default value is 64. |
| Connect through Bridges | Select this option to enable the client-bridge access point radio to associate with the infrastructure WLAN through another client-bridge radio thereby forming a chain. This is referred to as daisy chaining of client-bridge radios. This option is disabled by default. |
| Channel Dwell Time | Set the channel-dwell time from 50 to 2000 milliseconds. This is the time the client-bridge radio dwells on each channel (configured in the list of channels) when scanning for an infrastructure WLAN. The default is 150 milliseconds. |
| Authentication | Set the mode of authentication with the infrastructure WLAN. The authentication mode specified here should be the same as that configured on the infrastructure WLAN. The options are **None** and **EAP**. If you select **EAP**, specify the EAP authentication parameters. The default setting is *None*.<br>For information on WLAN authentication, see Configuring WLAN Security on page 556. |
| Encryption | Set the packet encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are **None**, **CCMP**, and **TKIP**. The default setting is *None*.<br>For information on WLAN encryption, see Configuring WLAN Security on page 556. |

3 Refer to the **EAP Parameters** field and define the following EAP authentication parameters:

| | |
|---|---|
| Type | Select the EAP authentication method used by the supplicant. The options are **TLS** and **PEAP-MS-CHAPv2**. The default EAP type is **PEAP-MS-CHAPv2**. |
| Username | Set the 32-character maximum user name for an EAP authentication credential exchange. |
| Password | Set the 32-character maximum password for the specified EAP user name. |
| Pre-shared Key | Set the PSK *(pre-shared key)* used with EAP. Note that the authenticating algorithm and PSK should be the same as on the infrastructure WLAN. |
| Handshake Basic Rate | Set the basic rate of exchange of handshake packets between the client-bridge and infrastructure WLAN Access Points. The options are **highest** and **normal**. The default value is **highest**. |

| | |
|---|---|
| Trustpoint CA | Set the *Trustpoint CA* name (this is the trustpoint installed on the RADIUS server host). This parameter is applicable to both EAP-TLS and PEAP-MS-CHAPv2 authentication modes.<br>In case of both EAP-TLS and PEAP-MS-CHAPv2 authentication, provide the RADIUS server TP name to enable RADIUS server certificate validation at the client end. This parameter is not mandatory for enabling TP-based authentication of CB *(Client-Bridge)* AP. |
| Trustpoint Client | Set the *Trustpoint Client* name (this is the TP installed on the CB AP). This parameter is applicable only for EAP-TLS authentication mode. When configured, this client certificate is sent across a TLS tunnel and matched for authentication at the RADIUS server host. This configuration is mandatory for enabling TP-based authentication of CB AP. |
| Trustpoint Expiry | Use the drop-down menu to specify whether the wireless client-bridge is to be continued or discontinued in case of certificate expiry.<br>In EAP-TLS authentication, a CA-signed certificate is used to authenticate the CB AP and RADIUS server host to establish the wireless CB. Use this option to specify whether the wireless CB is to be continued or terminated on expiration of this certificate.<br>**`continue`** – Enables continuation of the CB even after the certificate (CA/client) has expired. When selected, this option enables automatic CA certificate deployment as and when new CA certificates are available. This is the default setting.<br>**`discontinue`** – Terminates the CB once the certificate (CA/client) has expired.<br><br>Note:<br>Configure this parameter only if the CB AP and the RADIUS server host are using a crypto CMP policy for automatic certificate renewal. For more information, see Crypto CMP Policy on page 685. |

4 Refer to the **Channel Lists** field and define the list of channels the client-bridge radio scans when scanning for an infrastructure WLAN.

| | |
|---|---|
| Band A | Define a list of channels for scanning across all the channels in the 5.0 GHz radio band. |
| Band BG | Define a list of channels for scanning across all the channels in the 2.4 GHz radio band. |

5 Refer to the **Keepalive Parameters** field and define the following configurations:

| | |
|---|---|
| Keepalive Type | Set the keepalive frame type exchanged between the client-bridge and infrastructure access points. This is the type of packets exchanged between the client-bridge and infrastructure access points, at specified intervals, to keep the client-bridge link up and active. The options are **`null-data`** and **`WNMP`** packets. The default value is **`null-data`**. |
| Keepalive Interval | Set the keepalive interval from 0 to 86,400 seconds. This is the interval between two successive keepalive frames exchanged between the client-bridge and infrastructure Access Points. The default value is 300 seconds. |
| Inactivity Timeout | Set the inactivity timeout for each bridge MAC address from 0 to 864,000 seconds. This is the time for which the client-bridge access point waits before deleting a wired/wireless client's MAC address from which a frame has not been received for more than the time specified here. For example, if the inactivity time is set at 120 seconds, and if no frames are received from a client (MAC address) for 120 seconds, it is deleted. The default value is 600 seconds. |

6 Refer to the **Radio Link Behaviour** field and define the following configurations:

| | |
|---|---|
| Shutdown Other Radio when Link Goes Down | Select this option to enable shutting down of the non-client bridge radio (this is the radio to which wireless clients associate) when the link between the client-bridge and infrastructure access points is lost. When enabled, wireless clients associated with the non-client bridge radio are pushed to search for and associate with other access points having backhaul connectivity. This option is disabled by default.<br>If you enable this option, specify the time for which the non-client bridge radio is shut down. Use the spinner to specify a time from 1 - 1,800 seconds. |
| Refresh VLAN Interface when Link Comes Up | Select this option to enable the SVI to refresh on re-establishing client bridge link to the infrastructure access point. If you are using a DHCP assigned IP address, this option also causes a DHCP renew. This option is enabled by default. |

7 Refer to the **Roam Criteria** field and define the following configurations:

| | |
|---|---|
| Seconds for Missed Beacons | Set this interval from 0 to 60 seconds. This is the time for which the client-bridge access point waits, after missing a beacon from the associated infrastructure WLAN access point, before roaming to another infrastructure access point. For example, if Seconds for Missed Beacon is set to 30 seconds, and if more than 30 seconds have passed since the last beacon received from the infrastructure access point, the client-bridge access point resumes scanning for another infrastructure access point. The default value s 20 seconds. |
| Minimum Signal Strength | Set the minimum signal-strength threshold for signals received from the infrastructure access point. Specify a value from -128 to -40 dBm. If the RSSI value of signals received from the infrastructure access point falls below the value specified here, the client-bridge access point resumes scanning for another infrastructure access point. The default is -75 dBm. |

8 Click **OK** to save the changes and overrides to the client bridge settings screen.
Click **Reset** to revert to the last saved configuration.

### Advanced Settings

A radio's profile configuration is customizable to define how transmit and receive data frames are processed. A radio's sniffer redirect settings can be refined to adjust how captured packets are directed.

Additionally, channel scanning settings can refined in respect to channel scanning requirements on either the 2.4 or 5 GHz radio bands.

To set or edit the selected radio's advanced settings:

1 Select the **Advanced Settings** tab.

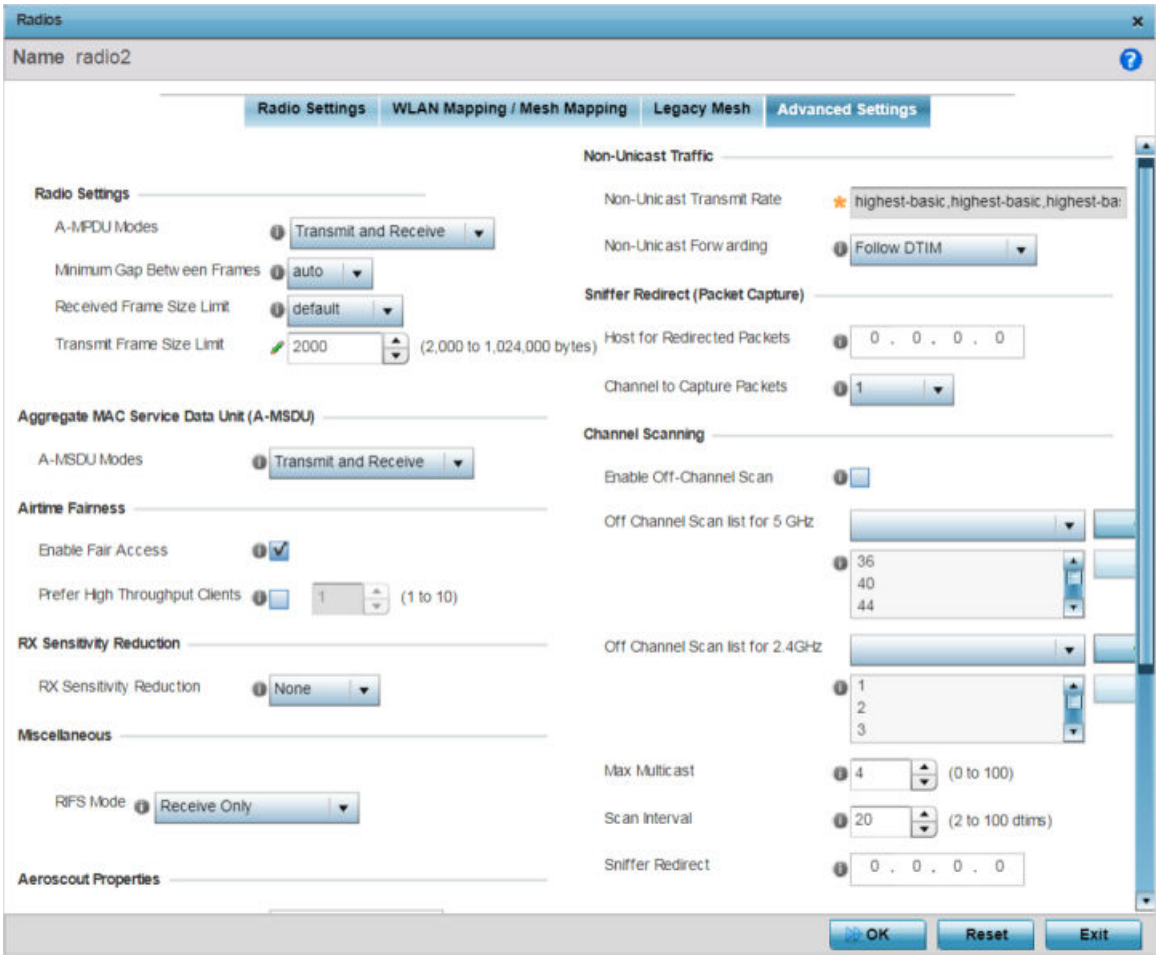



**Figure 40: Access Point - Radio Interface - Advanced Settings Screen**

2 Refer to the Radio Settings field to define how MAC service frames are aggregated by the access point radio.

| | |
|---|---|
| A-MPDU Modes | Use the drop-down menu to define the A-MPDU mode supported. Options include **Transmit Only**, **Receive Only**, **Transmit and Receive** and **None**. The default value is Transmit and Receive. Using the default value, long frames can be both sent and received (up to 64 KB). When enabled, define either a transmit or receive limit (or both). |
| Minimum Gap Between Frames | Use the drop-down menu to define, in microseconds, the minimum gap between consecutive A-MPDU frames. The options include:<br>• **0** – Configures the minimum gap as 0 microseconds<br>• **1** – Configures the minimum gap as 1 microseconds<br>• **2** – Configures the minimum gap as 2 microseconds<br>• **4** – Configures the minimum gap as 4 microseconds<br>• **8** – Configures the minimum gap as 8 microseconds<br>• **16** – Configures the minimum gap as 16 microseconds<br>• **auto** – Auto configures the minimum gap depending on the platform and radio type (default setting) |

| | |
|---|---|
| Received Frame Size Limit | If the A-MPDU mode is set to *Receive Only* or *Transmit and Receive*, use this option to define an advertised maximum limit for received A-MPDU aggregated frame size. The options include:<br>• **8191** - Advertises the maximum received frame size limit as 8191 bytes.<br>• **16383** - Advertises the maximum received frame size limit as 16383 bytes.<br>• **32767** - Advertises the maximum received frame size limit as 32767 bytes.<br>• **65535** - Advertises the maximum received frame size limit as 65535 bytes.<br>• **128000** - Advertises the maximum received frame size limit as 128000 bytes.<br>• **256000** - Advertises the maximum received frame size limit as 256000 bytes.<br>• **512000** - Advertises the maximum received frame size limit as 512000 bytes.<br>• **1024000** - Advertises the maximum received frame size limit as 1024000 bytes.<br>• **default** - This option auto configures the maximum received frame size based on the platform and radio type. This is the default setting. |
| Transmit Frame Size Limit | If the A-MPDU mode is set to *Transmit Only* or *Transmit and Receive*, use the spinner control to set limit on transmitted A-MPDU aggregated frame size. The range depends on the AP type and the radio selected.<br>For 802.11ac capable APs, the range is as follows:<br>• **2000 – 65,535 bytes** - For radio 1, the range is 2000 - 65,535 bytes. The default value is 65,535 bytes.<br>Note:<br>The WiNG *AP7662* and *AP7632* access points are an exception to the above rule. For the AP7662 and AP7632 access point models, the radio 1 range is *2000 - 1,024,000 bytes*. And the default value is 1,024,000 bytes.<br>• **2000 – 1,024,000 bytes** - For radio 2, the range is 2000 - 1,024,000 bytes. The default value is 1,024,000 bytes.<br>Note:<br>The WiNG 802.11ac capable APs are: AP7522, AP7532, AP7562, AP7602, AP7612, AP7632, AP7662, AP8432, and AP8533.<br>For non 802.11ac capable APs the range is as follows:<br>• **2000 – 65,535 bytes** - For both radio 1 and radio 2 the range is 2000 - 65,535 bytes. The default value is 65,535 bytes. |

3 in the Aggregate MAC Service Data Unit (A-MSDU) section , use the **A-MSDU Modes** drop-down menu to set the supported A-MSDU mode.

Available modes include **Receive Only** and **Transmit and Receive**. Transmit and Receive is the default value. Using Transmit and Receive, frames up to 4 KB can be sent and received. The buffer limit is not configurable.

4 Use the **Airtime Fairness** fields to optionally prioritize wireless access to devices.

| | |
|---|---|
| Enable Fair Access | Select this option to enable this feature and provide equal access client access to radio resources. |
| Prefer High Throughput Clients | Select this option to prioritize clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/ b/g) clients. Use the spinner control to set a weight for the higher throughput clients. |

5 Use the **Rx Sensitivity Reduction** drop-down menu to set the selected radio's receive sensitivity reduction threshold level.

This threshold determines the RSSI (in dBm) at which the radio acknowledges the SOP *(Start of Packet)* frames received from the client, and begins to demodulate and decode the packets.

In highly dense environments, or single-channel networks, having two or more radios sharing a channel, CCI *(co-channel interference)* adversely impacts network performance. By setting this threshold, you can control the radio's receive sensitivity to interference and noise, thereby reducing the impact of CCI. You are basically configuring the AP to not decode packets that have a signal strength below the specified threshold level.

The available *rx-sensitivity-reduction* threshold levels are: **`High`**, **`Low`**, **`Medium`** and **`None`**. Set the threshold level as *High*, to force your radio to ignore all traffic having a signal strength below the high threshold level value. This results in fewer traffic interruptions due to collision and Wi-Fi interference. Note, the default setting is *None*.

The following table provides the *rx-sensitivity-reduction threshold level* to *RSSI* mapping for the 2.4 GHz and 5 GHz bands:

| 802.11 Bands | High Threshold | Medium Threshold | Low Threshold |
|---|---|---|---|
| 2.4 GHz | -79 dBm | -82 dBm | -85 dBm |
| 5 GHz | -76 dBm | -78 dBm | -80 dBm |

Note

This feature is supported only on the following access points: AP-7522, AP 7532, AP 7562, AP-8432, AP-8533

6 Set the following **Aeroscout Properties**:

| | |
|---|---|
| Forward | Select enable to forward Aeroscout packets to a specified MAC address. Aeroscout tags associate with an access point, then communicate with a location engine. This setting is disabled by default. |
| MAC to be Forwarded | Specify the MAC address to be forwarded. |

7 Set the following **Ekahau Properties**:

| | |
|---|---|
| Forward Host | Specify the Ekahau engine IP address. Using Ekahau small, battery powered Wi-Fi tags are attached to tracked assets or carried by people. Ekahau processes locations, rules, messages and environmental data and turns the information into locationing maps, alerts and reports. |
| Forwarding Host | Use the spinner control to set the Ekahau TZSP port used for processing information from locationing tags. |
| MAC to be Forwarded | Specify the MAC address to be forwarded. |

8 Set the following **Non-Unicast Traffic** values for the profile's supported access point radio and its connected wireless clients:

| | |
|---|---|
| Broadcast/Multicast Transmit Rate | Use the drop-down menu to define the data rate broadcast and multicast frames are transmitted. Seven different rates are available if the not using the same rate for each BSSID, each with a separate menu. |
| Broadcast/Multicast Forwarding | Define whether client broadcast and multicast packets should always follow DTIM, or only follow DTIM when using Power Save Aware mode. The default setting is Follow DTIM. |

9 Refer to the **Sniffer Redirect (Packet Capture)** field to define the radio's captured packet configuration.

| | |
|---|---|
| Host for Redirected Packets | If packets are re-directed from a connected access point radio, define an IP address resource (additional host system) to capture the re-directed packets. This address is the numerical (non DNS) address of the host used to capture re-directed packets. |
| Channel to Capture Packets | Use the drop-down menu to specify the specific channel used to capture re-directed packets. The default value is channel 1. |

10 Refer to the **Channel Scanning** field to define the radio's captured packet configuration.

| | |
|---|---|
| Enable Off Channel Scan | Enable this option to scan across all channels using this radio. Channel scans use access point resources and can be time consuming, so only enable when your sure the radio can afford the bandwidth be directed towards to the channel scan and does not negatively impact client support. |
| Off Channel Scan list for 5GHz | Define a list of channels for off channel scans using the 5GHz access point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 5GHz radio band. |
| Off Channel Scan list for 2.4GHz | Define a list of channels for off channel scans using the 2.4GHz access point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 2.4GHz radio band. |
| Max Multicast | Set the maximum number (from 0 - 100) of multicast/broadcast messages used to perform off channel scanning. The default setting is four. |
| Scan Interval | Set the interval (from 2 - 100 dtims) off channel scans occur. The default setting is 20dtims. |
| Sniffer Redirect | Specify the IP address of the host to which captured off channel scan packets are redirected. |

11 Select **OK** to save the changes to the advanced settings screen. Select **Reset** to revert to the last saved configuration.

### *WAN Backhaul Configuration*

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a network device to connect, transmit and receive data over a Cellular Wide Area Network. The WWAN card uses *point to point protocol* (PPP) to connect to the *Internet Service Provider* (ISP) and gain access to the Internet. PPP is the protocol used for establishing internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

The following 3G cards are supported:

- Verizon V740
- Verizon PC770
- Sprint C777
- Novatel Merlin XU870
- Sierra Aircard 880E
- Telstra Elite Mobile Broadband
- Option GT Ultra Express
- Vodaphone Mobile Connect E3730
- Aircard 503
- Aircard 504 / AT & T 890

To define a WAN Backhaul configuration:

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Interface** menu and select **WAN Backhaul**.

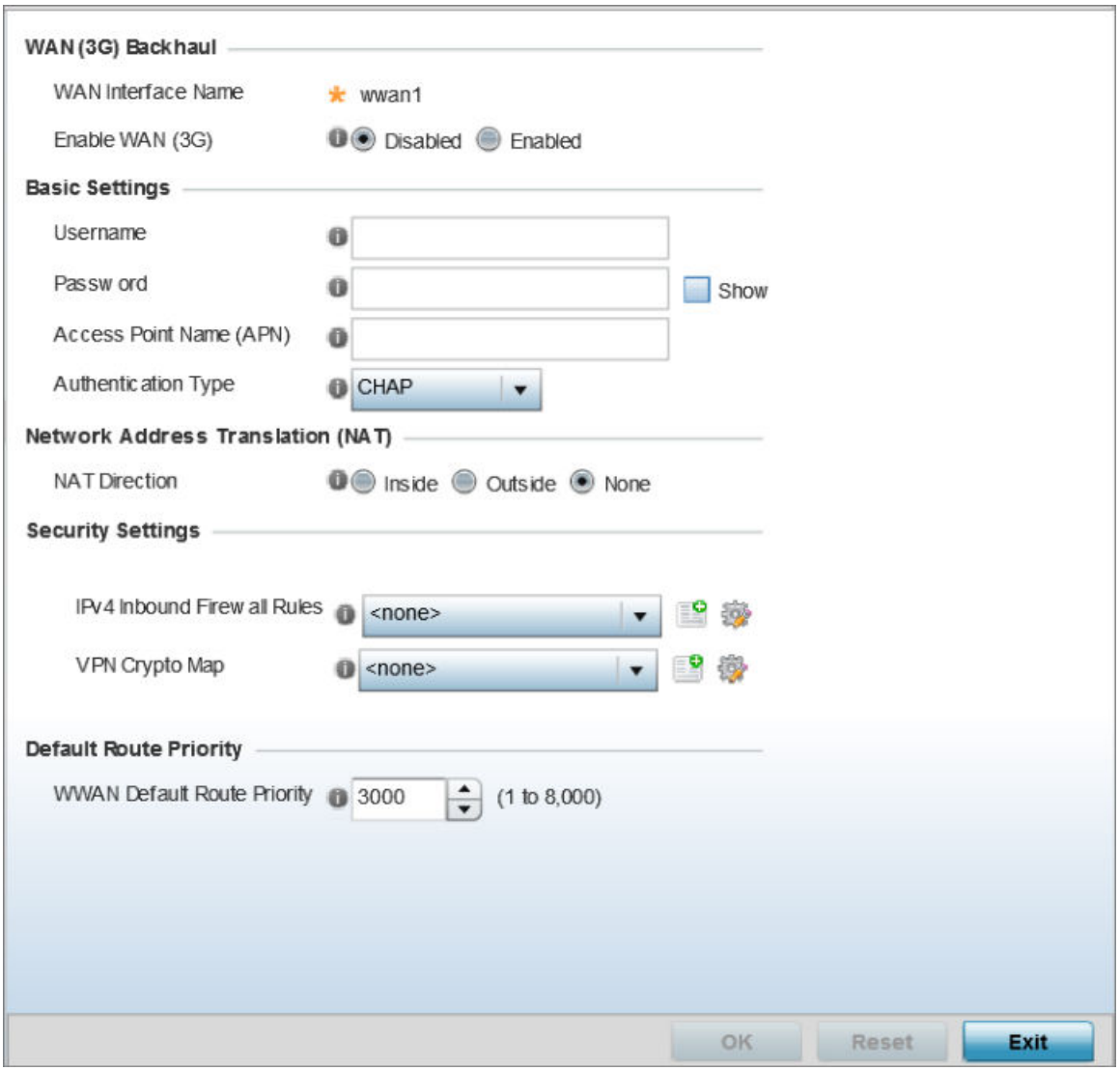



**Figure 41: Profile Interface - WAN Backhaul screen**

3 Refer to the WAN (3G) Backhaul configuration to specify the access point's WAN card interface settings:

| | |
|---|---|
| WAN Interface Name | Displays the WAN Interface name for the WAN 3G Backhaul card. |
| Enable WAN (3G) | Select this option to enable 3G WAN card support on the access point. A supported 3G card must be connected for this feature to work. |
| Username | Provide username for authentication support by the cellular data carrier. |
| Password | Provide password for authentication support by the cellular data carrier. |
| Access Point Name (APN) | Enter the name of the cellular data provider if necessary. This setting is needed in areas with multiple cellular data providers using the same protocols such as Europe, the Middle East and Asia. |

| | |
|---|---|
| Authentication Type | Use the drop-down menu to specify authentication type used by the cellular data provider. Supported authentication options include **None**, **PAP**, **CHAP**, **MSCHAP**, and **MSCHAP-v2**. |

4 Use the NAT Direction field to specify the NAT direction used with the access point's WAN card. Options include **Inside**, **Outside** or **None**. The default is None.

5 Configure the **IPv4 Inbound Firewall Rules**. Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the Create icon to define a new rule configuration or the Edit icon to modify an existing rule.

6 Select the **VPN Crypto Map** to use with this WWAN configuration. Use the drop-down menu to apply an existing crypto map configuration to this WWAN interface.

7 Use the **WWW Default Route Priority** spinner to set a default route priority for this interface. The default value is 3000.

8 Select **OK** to save the changes to the Advanced Settings screen. Select Reset to revert to the last saved configuration.

#### WAN Backhaul Deployment Considerations

Before defining a profile's WAN Backhaul configuration refer to the following deployment guidelines to ensure these configuration are optimally effective:

- If the WAN card does not connect after a few minutes after a no shutdown, check the access point's syslog for a *detected ttyUSB0 No such file* event. If this event has occurred, linux didn't detect the card. Re-seat the card.
- If the WAN card has difficulty connecting to an ISP (syslog shows that it retries LCP ConfReq for a long time), ensure the SIM card is still valid and is plugged in correctly.
- If a modem doesn't responding with an OK during the dialing sequence, the WAN card is in an unknown state and will not accept a command. Re-seat the card and begin the dialup sequence again until the card is recognized.
- If encountering a *panic* when conducting a hotplug, power off the access point for one minute. The access point could continue to panic or detect the descriptor of the last utilized WAN card. Thus, it's a good idea to clear the panic state by temporarily disconnecting then re-applying access point power.
- If wanting to unplug the WAN card, ensure sure you shutdown first, as the probability of getting a panic is reduced. With the new high-speed WAN cards currently being utilized, the chances of getting a panic significantly increase.

### *PPPoE Configuration*

*PPP over Ethernet* (PPPoE) is a data-link protocol for dialup connections. PPPoE allows the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol.

PPPoE enables controllers, service platforms, and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a

client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the access point's Wired WAN should fail.

Note

PPPoE-enabled devices continue to support VPN, NAT, PBR, and 3G failover on the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

When PPPoE client operation is enabled, it discovers an available server and establishes a PPPoE link for traffic slow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, traffic is redirected back through the access point's wired WAN link.

When the access point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

Note

The WiNG 7.1 releases does not provide PPPoE support on the AP505 and AP510 model access points. This feature will be supported in future releases.

To create a PPPoE point-to-point configuration:

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Interface** menu and select **PPPoE**.

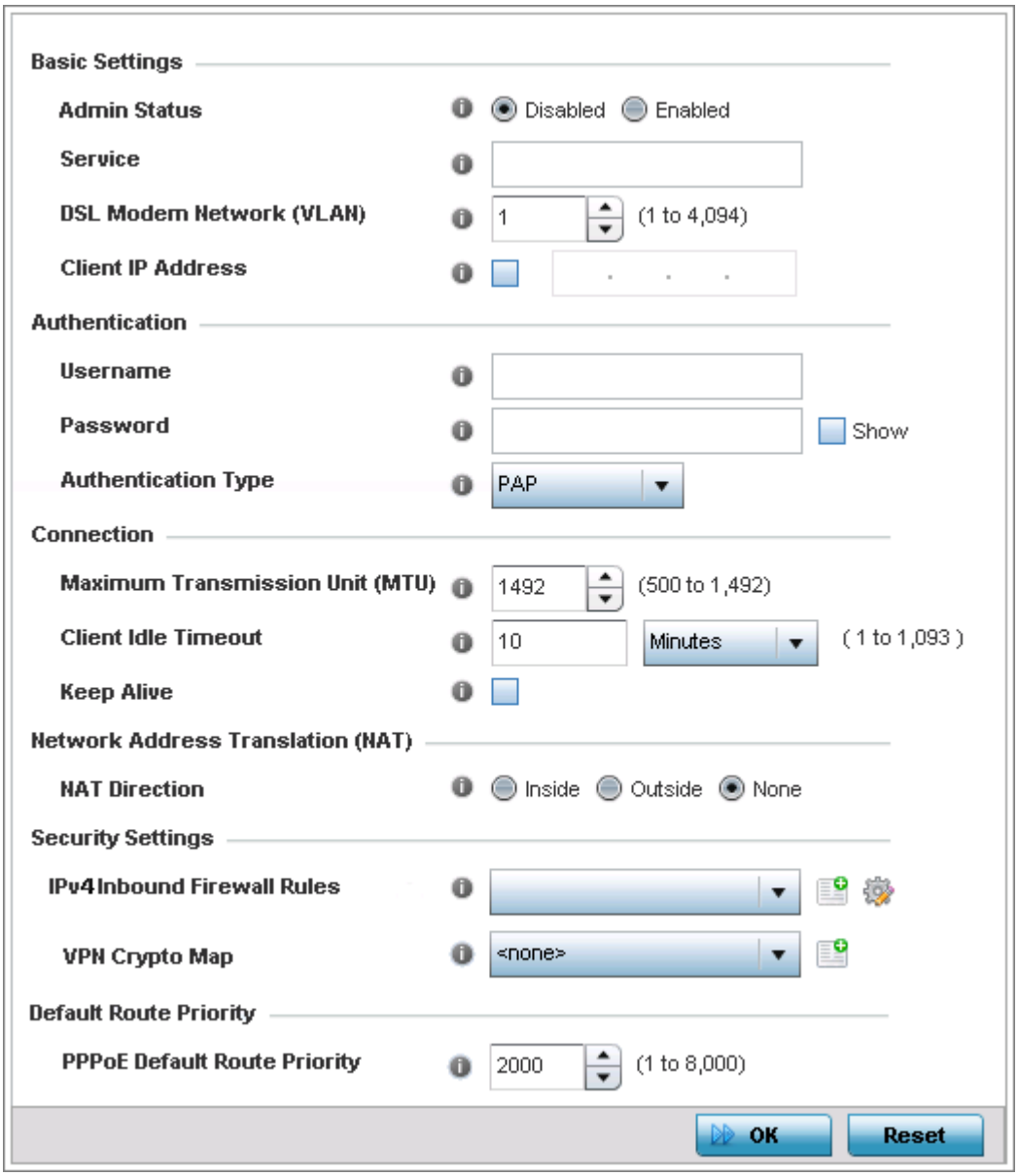



**Figure 42: Profile Interface - PPPoE screen**

3 Use the Basic Settings field to enable PPPoE and define a PPPoE client.

| | |
|---|---|
| Enable PPPoE | Select this option to support a high speed client mode point-to-point connection using the PPPoE protocol. The default setting is disabled. |
| Service | Enter the 128-character maximum PPPoE client service name provided by the service provider. |
| DSL Modem Network (VLAN) | Set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to the DSL modem. The available range is 1 - 4,094. The default value is 1. |
| Client IP Address | Provide the numerical (non hostname) IP address of the PPPoE client. |

4 Define the following **Authentication** parameters for PPPoE client interoperation:

| | |
|---|---|
| Username | Provide the 64 character maximum username used for authentication support by the PPPoE client. |
| Password | Provide the 64 character maximum password used for authentication by the PPPoE client. Click **Show** to display the characters that make up the password. |
| Authentication Type | Specify the authentication type used by the PPPoE client, and whose credentials must be shared by its peer access point. Supported authentication options include **`None`**, **`PAP`**, **`CHAP`**, **`MSCHAP`**, and **`MSCHAP-v2`**. |

5 Define the following **Connection** settings for the PPPoE point-to-point connection with the PPPoE client:

| | |
|---|---|
| Maximum Transmission Unit (MTU) | Set the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492. |
| Client Idle Timeout | Set a timeout in either **`Seconds`** (1 - 65,535), **`Minutes`** (1 - 1,093) or **`Hours`** (1-18). The access point uses the defined timeout so it does not sit idle waiting for input from the PPPoE client and server that may never come. The default setting is 10 minutes. |
| Keep Alive | Select this option to ensure that the point-to-point connection to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default. |

6 Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

NAT converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point router maps its local (**`Inside`**) network addresses to WAN (**`Outside`**) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. The default setting is **`None`** (neither inside nor outside).

7 Define the following **Security Settings** for the PPPoE configuration:

| | |
|---|---|
| Inbound IP Firewall Rules | Select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If there is no firewall rule that meets the data protection needs of the PPPoE client connection, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing rule. For more information, see Wireless Firewall on page 730. |
| VPN Crypto Map | Use the drop-down menu to apply an existing crypto map configuration to this PPPoE interface. |

8 Set the **Default Route Priority** for the default route learned using PPPoE.

Select from 1 - 8,000. The default setting is 2,000.

9 Click **OK** to save the changes and overrides made to the **PPPoE** screen.

Click **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

### *Bluetooth Configuration*

The AP7602, AP7612, AP7632, AP7662, AP8432 and AP8533 model access points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network.

AP-8432 and AP-8533 models support both Bluetooth classic and Bluetooth low energy technology.

These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

BLE enabled access points support Bluetooth beaconing to emit either iBeacon or Eddystone- URL beacons. The access point's Bluetooth radio sends non-connectable, undirected low-energy (LE) advertisement packets on a periodic basis. These advertisement packets are short, and they are sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. Portions of the advertising packet are still customizable, however.

Note
The WiNG 7.1 release does not provide Bluetooth support on AP505i and AP510i model access points. This feature will be supported in future releases.

To define a Bluetooth radio interface configuration:

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Interface** menu and select **Bluetooth**.

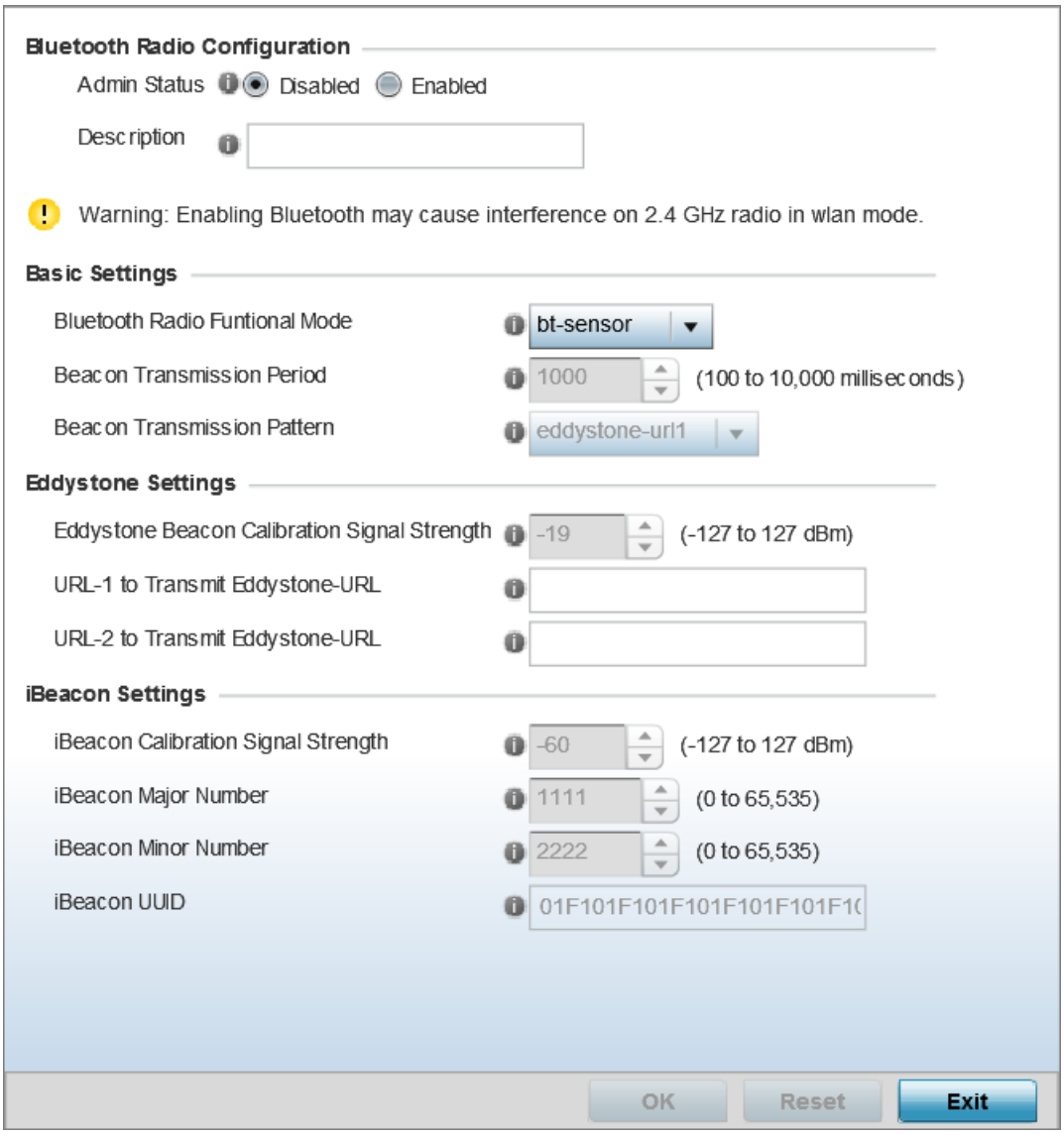



**Figure 43: Profile Interface - Bluetooth Screen**

3 Set the following Bluetooth Radio Configuration parameters:

| | |
|---|---|
| Admin Status | **`Enable`** or **`Disable`** Bluetooth support capabilities for the access point radio transmissions.<br>The default value is disabled. |
| Description | Define a 64 character maximum description for the access point's Bluetooth radio to differentiate this radio interface from other Bluetooth supported radio's that might be members of the same RF Domain. |

4 Set the following **Basic Settings**:

| | |
|---|---|
| Bluetooth Radio Functional Mode | Set the access point's Bluetooth radio functional mode to either **`bt-sensor`**, **`le-beacon`**, **`le-tracking`** or **`le-sensor`**.<br>• bt-sensors are Bluetooth classic sensors providing robust wireless connections for legacy devices. Typically these connections are not ideally suited for the newer Bluetooth low energy technology supported devices.<br>• le-beacons are newer Bluetooth low energy beacons ideal for applications requiring intermittent or periodic transfers of small amounts of data. le-beacons are not designed as replacements for classic beacon sensors. The *bt-sensor* option is the default setting.<br><br>Note: Setting the Bluetooth Radio Functional mode to 'le-beacon' enables the '**`Beacon Transmission Period`**' and '**`Beacon Transmission Pattern`**' options. |
| Beacon Transmission Period | Set the Bluetooth radio's beacon transmission period from 100 - 10,000 milliseconds. As the defined period increases, so does the CPU processing time and the number packets incrementally transmitted (typically one per minute). The default setting is 1,000 milliseconds. |
| Beacon Transmission Pattern | When the Bluetooth radio's mode is set to **`le-beacon`**, use the enabled drop-down menu to set the beacon's emitted transmission pattern to **`eddystone_url1`**, **`eddystone_url2`**, or **`ibeacon`**.<br>An eddystone-URL frame broadcasts a URL using a compressed encoding scheme to better fit within a limited advertisement packet. Once decoded, the URL can be used by a client for internet access. If an eddystone-URL beacon broadcasts `https:anysite`, then clients receiving the packet can access that URL.<br>iBeacon was created by Apple for use in iOS devices (beginning with iOS version 7.0). Apple has made three data fields available to iOS applications: a UUID for device identification, a Major value for device class, and a Minor value for more refined information like product category. |

5 Define the following Eddystone Settings if you have set the **Beacon Transmission Pattern** to either **`eddystone_url1`** or **`eddystone_url2`**:

| | |
|---|---|
| Eddystone Beacon Calibration Signal Strength | Set the Eddystone Beacon measured calibration signal strength, from -127 dBm to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters. The default setting is -19 dBm. |
| URL-1 to Transmit Eddystone-URL | Enter a 64-character maximum Eddystone-URL1. The URL must be 18 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a web server. |
| URL-2 to Transmit Eddystone-URL | Enter a 64-character maximum Eddystone-URL2. The URL must be 18 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a web server. |

6 Define the following **iBeacon Settings** if you have set the **Beacon Transmission Pattern** to **ibeacon**:

| | |
|---|---|
| Beacon Calibration Signal Strength | Set the iBeacon measured calibration signal strength, from -127 dBm to 127 dBm, at 1 meter. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 1 meter. The default setting is -60 dBm. |
| iBeacon Major Number | Set the iBeacon major value from 0 - 65, 535. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. The default value is 1,111. |
| iBeacon Minor Number | Set the iBeacon minor value from 0 - 65, 535. Minor values identify and distinguish individual beacons. Minor values help identify individual beacons within a group of beacons assigned a major value. The default setting is 2,222. |
| iBeacon UUID | Define a 32 hex character maximum *Universally Unique IDentifier* (UUID). The UUID classification contains 32 hexadecimal digits, split into 5 groups, separated by dashes – for example, `f2468da6-5fa8-2e84-1134- bc5b71e0893e`. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration. |

7 Select **OK** to save the changes to the Bluetooth configuration.

Select **Reset** to revert to the last saved configuration. Saved configurations persist across reloads.

## Profile Network Configuration

Setting an access point profile's network configuration is a large task comprised of numerous administration activities.

Before defining a profile's network configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Administrators often need to route traffic to interoperate between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception.
- Static routes, while easy, can be overwhelming within a large or complicated network. Each time there is a change, someone must manually make changes to reflect the new route. If a link goes down, even if there is a second path, the router would ignore it and consider the link down.
- Static routes require extensive planning and have a high management overhead. The more routers that exist in a network, the more routes need to be configured. If you have N number of routers and a route between each router is needed, then you must configure N x N routes. Thus, for a network with nine routers, you will need a minimum of 81 routes (9 x 9 = 81).

An access point profile network configuration process consists of the following:


- DNS Configuration on page 146
- ARP Configuration on page 148
- L2TPv3 Configuration on page 149
- GRE Tunnel Configuration on page 158

*DNS Configuration*

DNS *(Domain Name System)* is a hierarchical naming system for resources connected to the Internet or a private network. Primarily, DNS resources translate domain names into IP addresses. If one DNS server doesn't know how to translate a particular domain name, it asks another one until the correct IP address is returned. DNS enables access to resources using human friendly notations. DNS converts human friendly domain names into notations used by different networking equipment for locating resources.

As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS, in the simplest terms, you would need to remember a series of numbers (123.123.123.123) instead of an easy to remember domain name (for example, *www.domainname.com*).

To define the DNS configuration:

1 Go to **Configuration → Devices → System Profile** .

The AP's Profile configuration menu displays.

2 Expand the **Network** menu and select **DNS**.

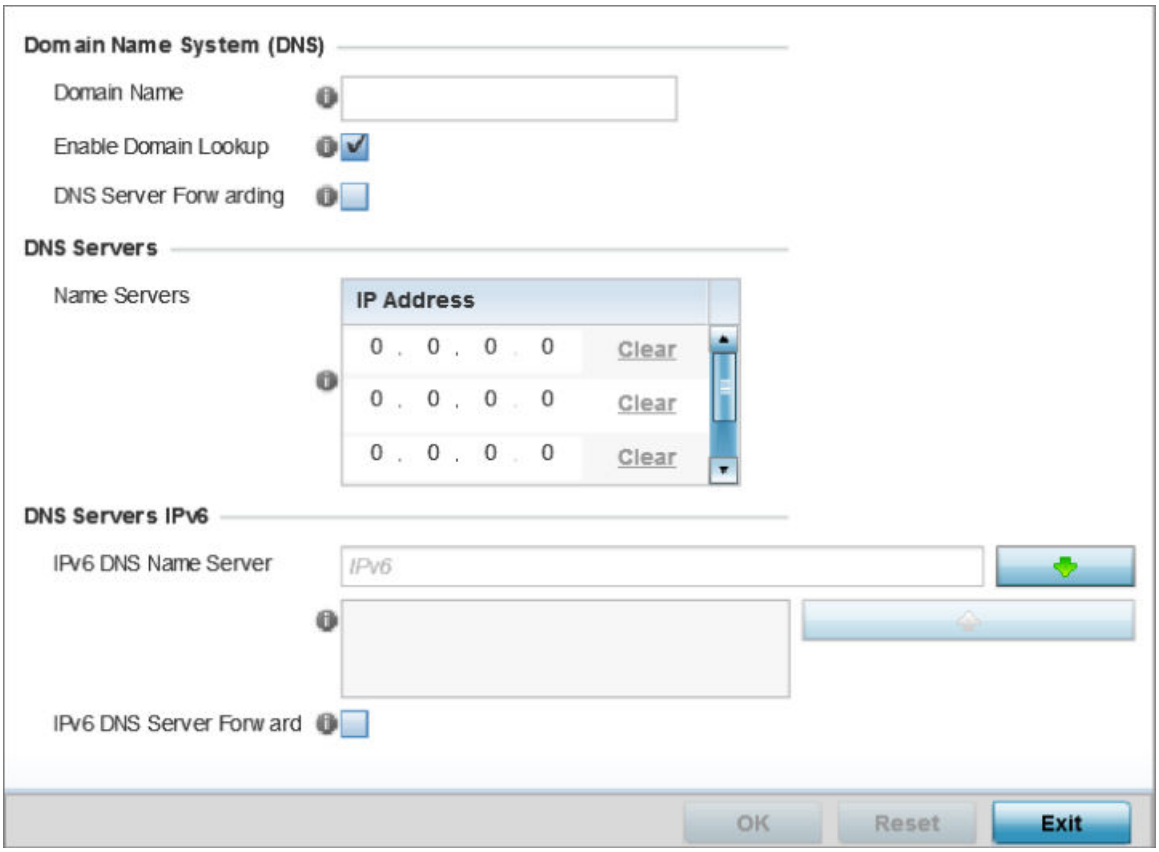



**Figure 44: Network - DNS Screen**

3 Set the following Domain Name System (DNS) configuration data:

| | |
|---|---|
| Domain Name | Provide the default Domain Name used to resolve DNS names. The name cannot exceed 64 characters. |
| Enable Domain Lookup | Select the check box to enable DNS. When enabled, human friendly domain names are converted into numerical IP destination addresses. The radio button is selected by default. |
| DNS Server Forwarding | Select this option to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by local DNS resources. This feature is disabled by default. |

4 In the **Name Servers** field, provide the IP addresses of up to three DNS server resources available to the access point.

5 Set the following DNS Servers IPv6 configuration data when using IPv6:

| | |
|---|---|
| IPv6 DNS Name Server | Provide the default domain name used to resolve IPv6 DNS names. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted. |
| IPv6 DNS Server Forward | Select the check box to enable IPv6 DNS domain names to be converted into numerical IP destination addresses. The setting is disabled by default. |

6 Click **OK** to save the changes made to the DNS configuration.

Click **Reset** to revert to the last saved configuration.

*ARP Configuration*

ARP *(Address Resolution Protocol)* is a protocol for mapping an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, ARP is used to find a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to see if a device knows it has that IP address associated with it. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

To define an ARP supported configuration:

1 Go to **Configuration → Devices → System Profile** tab from the Web UI.
The Profile screen displays. This screen lists access point profiles supported by the logged device.

2 Select a profile from the list.
The selected profile's configuration menu displays.

3 Expand the **Network** node and select **ARP**.

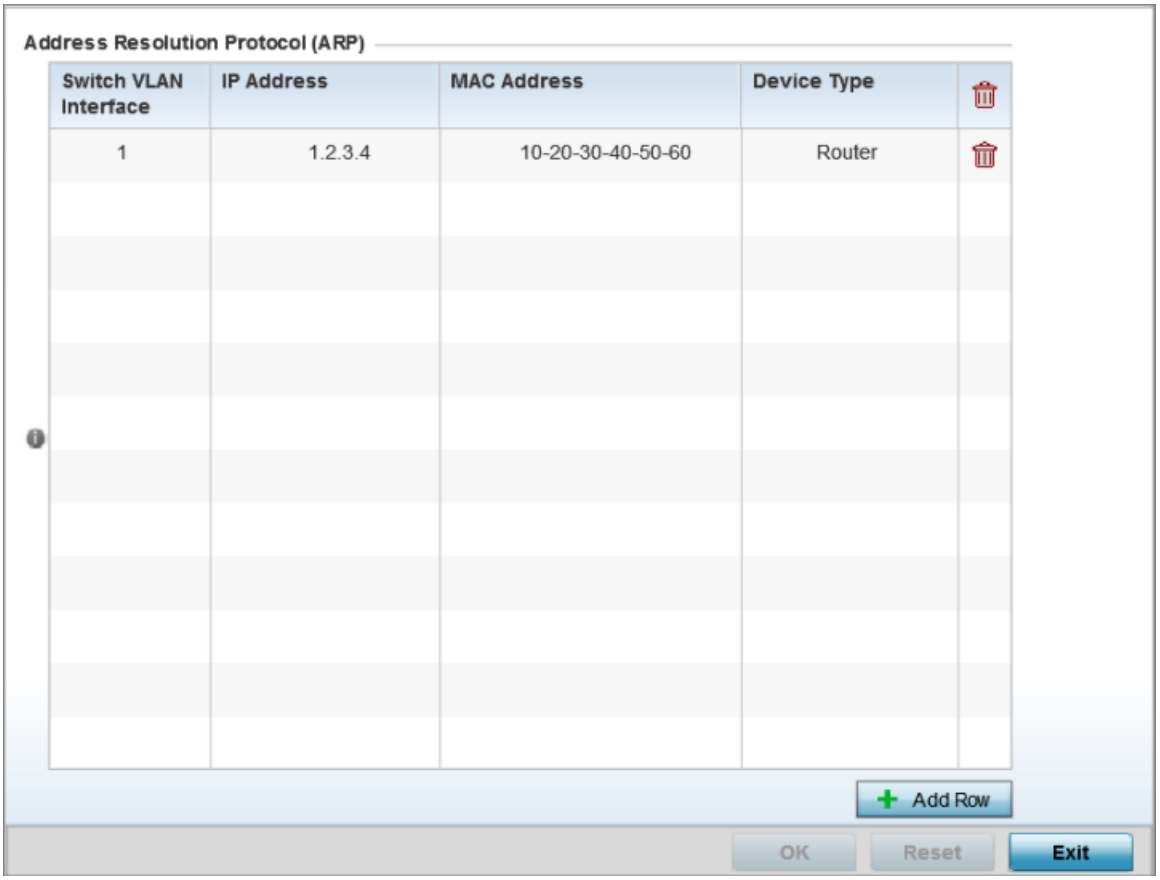



**Figure 45: Network - ARP screen**

4 Select **+ Add Row** from the lower right-hand side of the screen to populate the ARP table with rows used to define ARP network address information.

5 Set the following parameters to define the ARP configuration:

| | |
|---|---|
| Switch VLAN Interface | Use the spinner control to select a virtual interface for an address requiring resolution with the controller, service platform or access point. |
| IP Address | Define the IP address used to fetch a MAC Address recognized on the wireless network. |
| MAC Address | Displays the target MAC address subject to resolution. This is the MAC used for mapping an IP address to a MAC address recognized on the network. |
| Device Type | Specify the device type the ARP entry supports. Host is the default setting. |

6 Click the **OK** button located at the bottom right of the screen to save the changes to the ARP configuration.

Click **Reset** to revert to the last saved configuration.

### *L2TPv3 Configuration*

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and profile). L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables controllers, service platforms and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WiNG managed devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. access points support an Ethernet VLAN pseudowire type exclusively.

Note
A pseudowire is an emulation of a layer 2 point-to-point connection over a PSN *(packet-switching network)*. A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-

alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

**Note**
If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

**Note**
WiNG 7.1 release does not support L2TPv3 tunneling on AP505i and AP510i model access points. This feature will be supported in future releases.

To define an L2TPV3 configuration:

1 Go to **Configuration → Devices → System Profile** .

The Profile screen displays. This screen lists access point profiles.

2 Select a profile from the list.

The selected profile's configuration menu displays.

3 Expand the **Network** node and select **L2TPv3**.

The L2TPv3 General configuration screen displays by default.

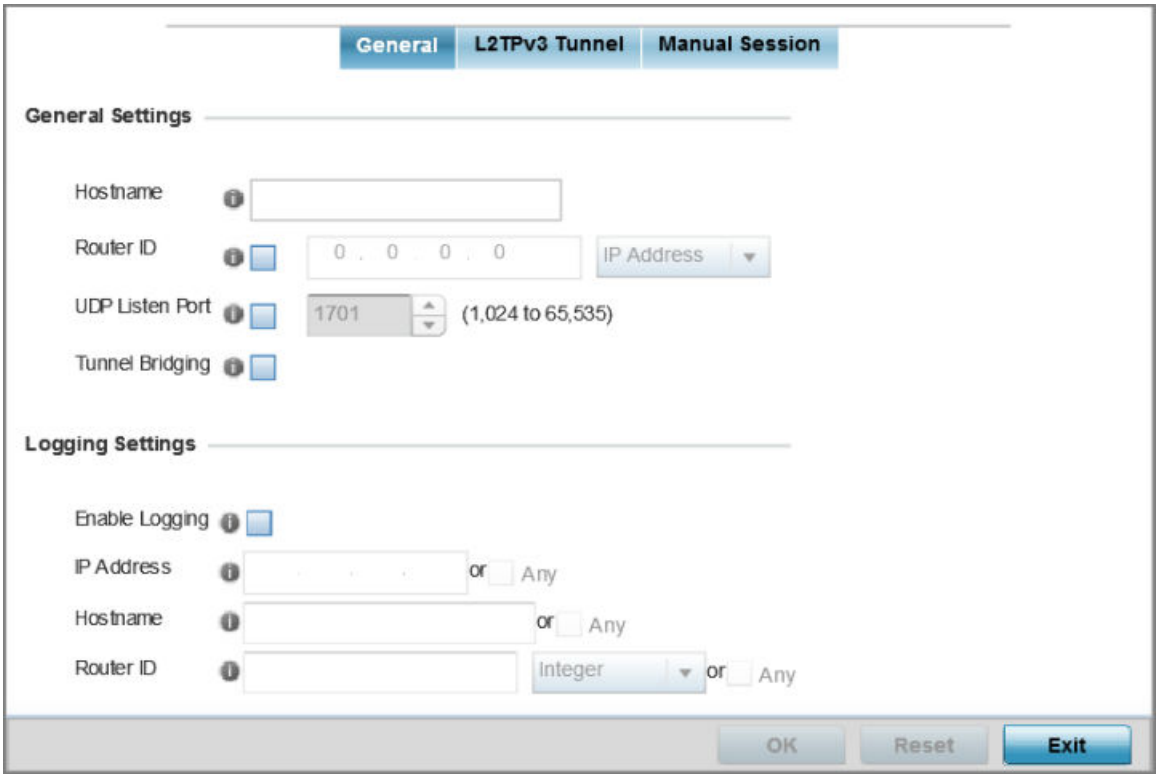



**Figure 46: Network - L2TPv3 screen - General tab**

4 In the General Settings field, configure the following settings:

| | |
|---|---|
| Host Name | Define a 64 character maximum hostname to specify the name of the host that's sent tunnel messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host. |
| Router ID | Set either the numeric IP address or the integer used as an identifier for tunnel AVP messages. AVP messages assist in the identification of a tunneled peer. |
| UDP Listen Port | Select this option to set the port used for listening to incoming traffic. Select a port from 1,024 - 65,535. The default port is 1701. |
| Tunnel Bridging | Select this option to enable or disable bridge packets between two tunnel end points. This setting is disabled by default. |

5 In the Logging Settings filed, configure the following settings:

| | |
|---|---|
| Enable Logging | Select this option to enable the logging of Ethernet frame events to and from bridge VLANs and physical ports on a defined IP address, host or router ID. This setting is disabled by default. |
| IP Address | Optionally use a peer tunnel ID address to capture and log L2TPv3 events. |
| Hostname | If not using an IP address for event logging, optionally use a peer tunnel hostname to capture and log L2TPv3 events. |
| Router ID | If not using an IP address or a hostname for event logging, use a router ID to capture and log L2TPv3 events. |

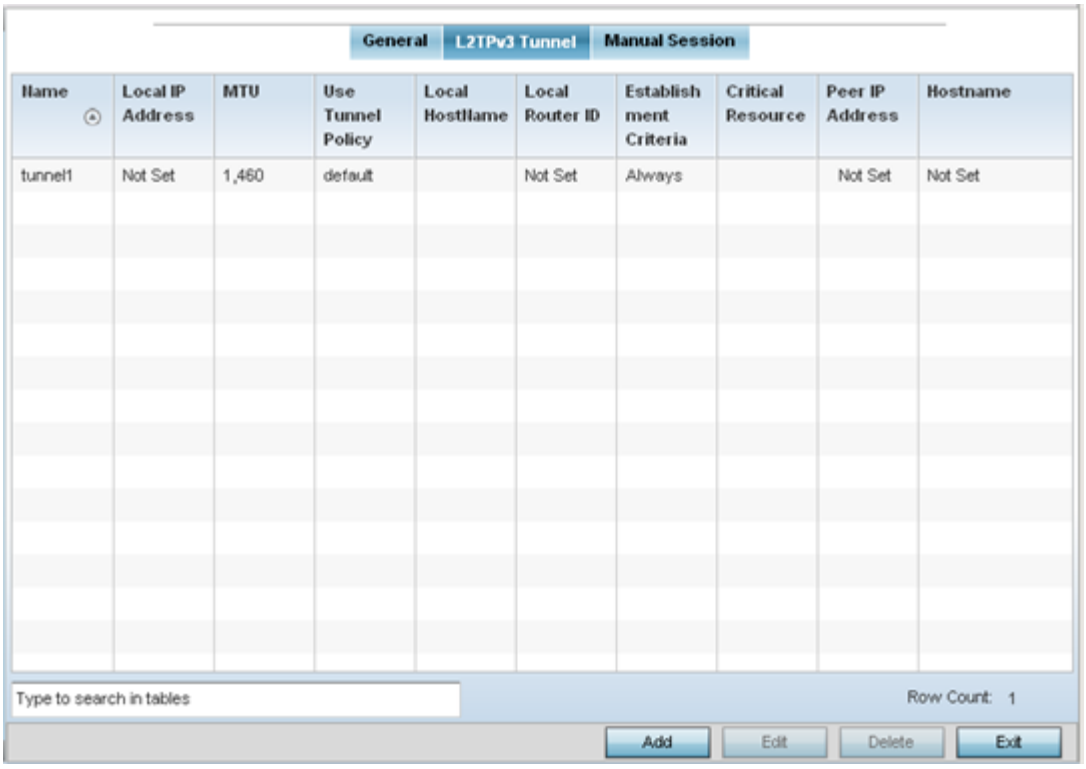
6 Select **OK** to save the changes to the session configuration.

Select **Reset** to revert to the last saved configuration.

### L2TPV3 Tunnel

To define an L2TPV3 configuration for a profile:

1 Select the **L2TPv3 Tunnel** tab.




2 Review the following L2TPv3 tunnel configuration data:

| | |
|---|---|
| Name | Displays the name of each listed L2TPv3 tunnel assigned upon creation. |
| Local IP Address | Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. |
| MTU | Displays the MTU *(maximum transmission unit)* size for each listed tunnel. The MTU is the size (in bytes) of the largest protocol data unit that the layer can pass between tunnel peers. |
| Use Tunnel Policy | Lists the L2TPv3 tunnel policy assigned to each listed tunnel. |
| Local Hostname | Lists the tunnel specific hostname used by each listed tunnel. This is the host name advertised in tunnel establishment messages. |
| Local Router ID | Specifies the router ID sent in the tunnel establishment messages. |

3 Either select **Add** to create a new L2TPv3 tunnel configuration, **Edit** to modify an existing tunnel configuration or **Delete** to remove a tunnel from those available to this profile.

Adding and Editing L2TPV3 Tunnels

You can add a new L2TPv3 tunnel configuration or edit an existing configuration.

1 Select **Add** to create a new L2TPv3 tunnel configuration, **Edit** to modify an existing tunnel configuration or **Delete** to remove a tunnel from those available to this profile.

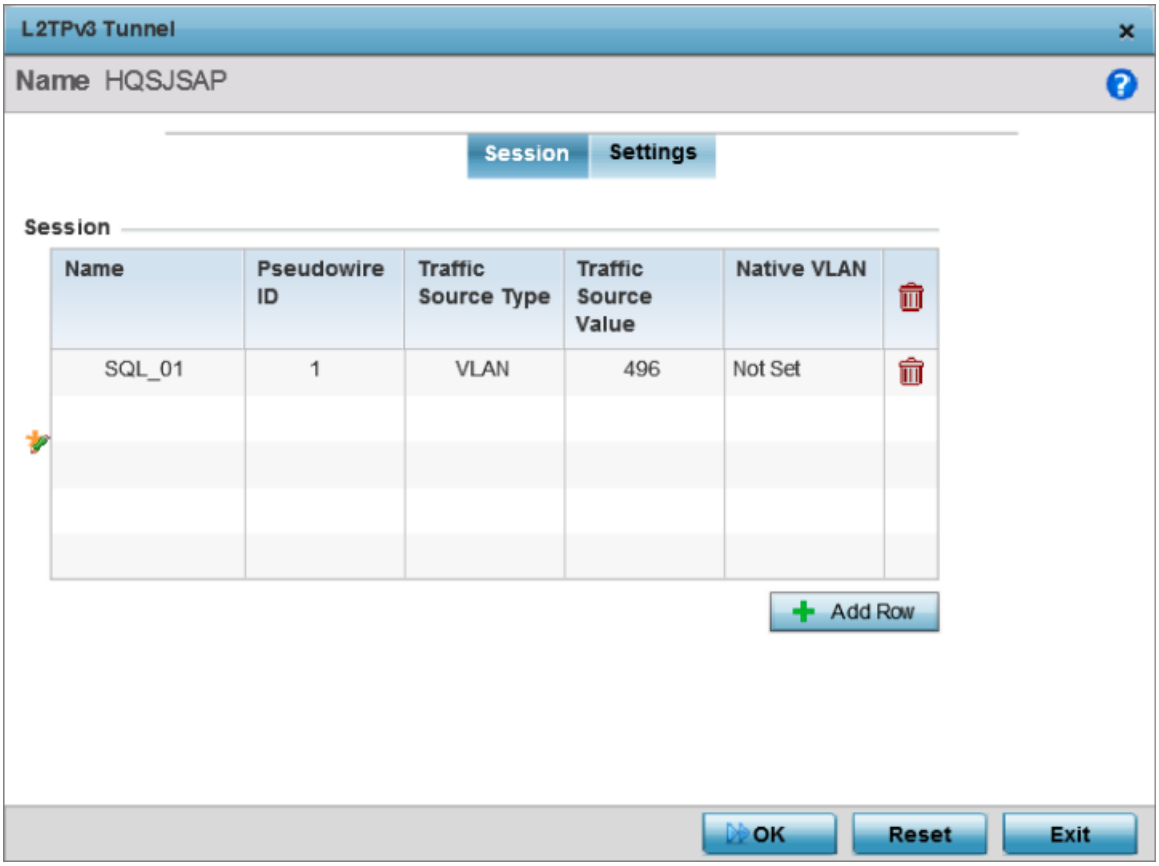



**Figure 47: L2TPv3 Tunnel - Session Configuration Screen**

2 If creating a new tunnel configuration, assign it a 32 character maximum **Name**.

3 Refer to the Session table to review the configurations of the peers available for tunnel connection. Select **+ Add Row** and provide the following L2TPv3 session settings:

| | |
|---|---|
| Name | Enter a 31 character maximum session name. There is no idle timeout for a tunnel. A tunnel is not usable without a session and a subsequent session name. The tunnel is closed when the last session tunnel session is closed. |
| Pseudowire ID | Define a psuedowire ID for this session. A pseudowire is an emulation of a layer 2 point-to-point connection over a PSN. A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network. |
| Traffic Source Type | Lists the type of traffic tunneled in this session (VLAN, etc.). |
| Traffic Source Value | Define a VLAN range to include in the tunnel session. Available VLAN ranges are from 1 - 4,094. |
| Native VLAN | Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer. |

4 Define the following **Settings** required for the L2TP tunnel configuration:

| | |
|---|---|
| Local IP Address | Enter the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the tunnel and responding to incoming tunnel create requests. |
| MTU | Set the MTU *(maximum transmission unit)*. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers. Define a MTU from 128 - 1,460 bytes. The default setting is 1,460. A larger MTU means processing fewer packets for the same amount of data. |
| Use Tunnel Policy | Select the L2TPv3 tunnel policy. The policy consists of user defined values for protocol specific parameters which can be used with different tunnels. If none is available, a new policy can be created or an existing one can be modified. |
| Local Hostname | Provide the tunnel specific hostname used by this tunnel. This is the host name advertised in tunnel establishment messages. |
| Local Router ID | Specify the router ID sent in tunnel establishment messages with a potential peer device. |

5 Define the following Rate Limit settings:

Rate limiting manages the maximum rate sent to or received from L2TPv3 tunnel members.

| | |
|---|---|
| Session Name | Use the drop-down menu to select the tunnel session that will have the direction, burst size and traffic rate settings applied. |
| Direction | Select the direction for L2TPv3 tunnel traffic rate limiting. Egress traffic is outbound L2TPv3 tunnel data coming to the controller, service platform or access point. Ingress traffic is inbound L2TPv3 tunnel data coming to the controller, service platform or access point. |
| Max Burst Size | Set the maximum burst size for egress or ingress traffic rate limiting (depending on which direction is selected) on a L2TPv3 tunnel. Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for L2TPv3 tunnel traffic. The default setting is 320 bytes. |
| Rate | Set the data rate (from 50 - 1,000,000 kbps) for egress or ingress traffic rate limiting (depending on which direction is selected) for an L2TPv3 tunnel. The default setting is 5000 kbps. |
| Background | Set the random early detection threshold in % for background traffic. Set a value from 1 - 100%. The default is 50%. |
| Best-Effort | Set the random early detection threshold in % for best-effort traffic. Set a value from 1 - 100%. The default is 50%. |
| Video | Set the random early detection threshold in % for video traffic. Set a value from 1 - 100%. The default is 25%. |
| Voice | Set the random early detection threshold in % for voice traffic. Set a value from 1 - 100%. The default is 25%. |

6 Review the Peer configurations. Select **+ Add Row** and configure a maximum of two peer configurations. Define the following **Peer** parameters:

| | |
|---|---|
| Peer ID | Define the primary peer ID used to set the primary and secondary peer for tunnel fail over. If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this access point, it creates the tunnel if the hostname and/or Router ID matches. |
| Router ID | Specify the router ID sent in tunnel establishment messages with this specific peer. |
| Hostname | Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process. |
| Encapsulation | Select either **IP** or **UDP** as the peer encapsulation protocol. UDP uses a simple transmission model without implicit handshakes. The default setting is *IP*. |
| Peer IP Address | Select this option to enter the numeric IP address used as the destination peer address for tunnel establishment. |
| UDP Port | If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. |
| IPSec Secure | Enable this option to enable security on the connection between the access point and the Virtual Controller. |
| IPSec Gateway | Specify the IP Address of the IPSec Secure Gateway. |

7 Define the following Fast Failover parameters:

| | |
|---|---|
| Enable | When enabled, the device starts sending tunnel requests on both peers, and in turn, establishes the tunnel on both peers. If disabled, tunnel establishment only occurs on one peer, with failover and other functionality the same as legacy behavior. If fast failover is enabled after establishing a single tunnel the establishment is restarted with two peers. One tunnel is defined as active and the other as standby. Both tunnels perform connection health checkups with individual hello intervals. This setting is disabled by default. |
| Enable Aggressive Mode | When enabled, tunnel initiation hello requests are set to zero. For failure detections, hello attempts are not retried, regardless of defined retry attempts. This setting is disabled by default. |

8 Select OK to save the changes within the L2TP Tunnel screen. Select Reset to revert the screen to its last saved configuration.

**Manual Session**

After a successful tunnel connection and establishment, individual sessions can be created. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

To define an L2TPv3 manual session configuration for a profile:

1 Select the **Manual Session** tab.

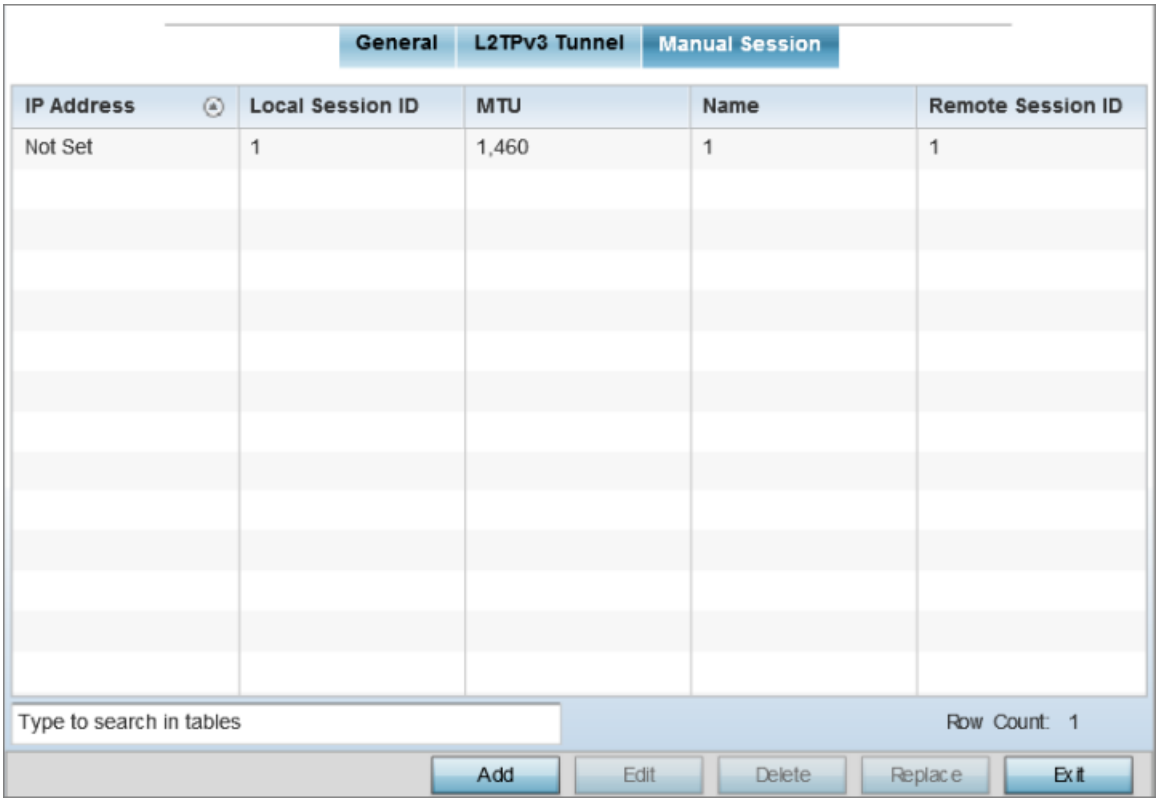



**Figure 48: L2TPv3 Tunnel - Manual Session Configuration Screen**

2 Refer to the following manual session configurations to determine whether one should be created or modified:

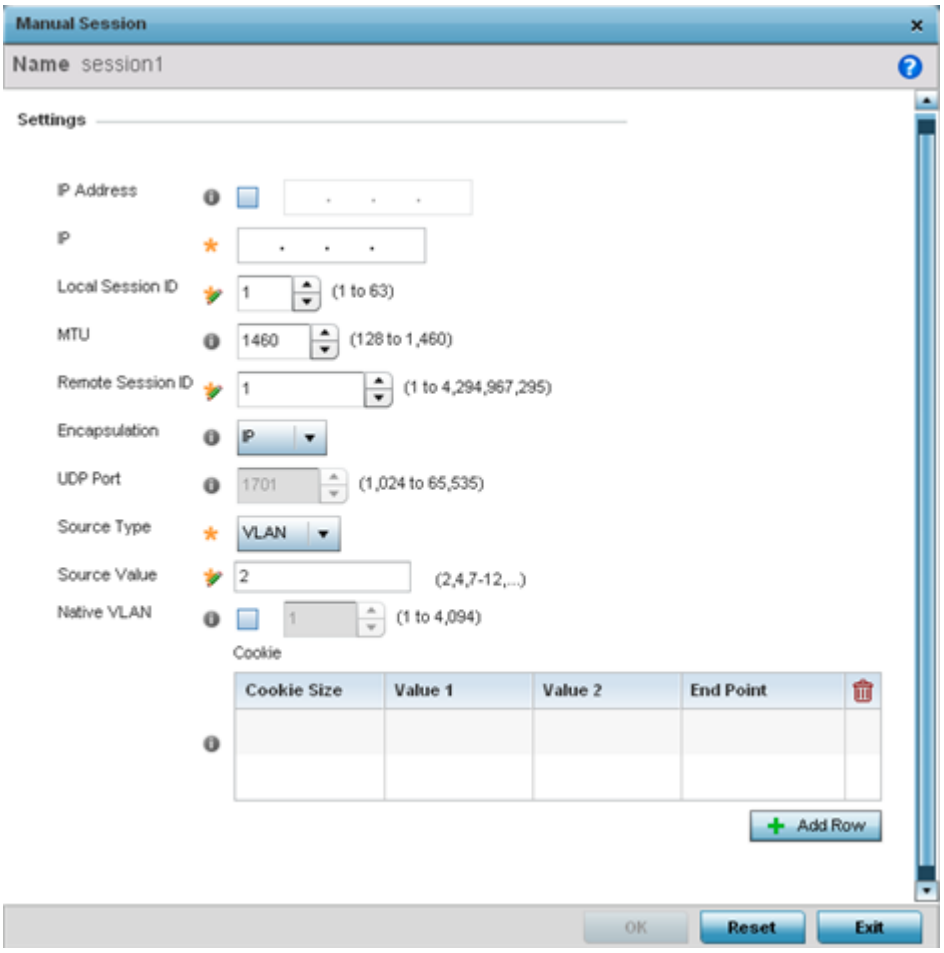
| | |
|---|---|
| IP Address | Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the tunnel session and responding to incoming requests. |
| Local Session ID | Displays the numeric identifier assigned to each listed tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer. |
| MTU | Displays each session's MTU. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data. |
| Name | Lists the name assigned to each listed manual session. |
| Remote Session ID | Lists the remote session ID passed in the establishment of the tunnel session. |

3 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

Adding and Editing Manual Sessions

You can add a new L2TPv3 manual session configuration or edit an existing configuration.

1 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.




2 Set the following manual session **Settings** parameters:

| | |
|---|---|
| Name | If creating a new manual session, define a 31 character maximum name for this tunnel session. The session is created after a successful tunnel connection and establishment. Each session name represents a single data stream. |
| IP Address | Specify the IP address used as the tunnel source IP address. If not specified, the tunnel source IP address is selected automatically based on the tunnel peer IP address. This address is applicable only for initiating the tunnel. When responding to incoming tunnel create requests, it would use the IP address received in the tunnel creation request. |
| IP | Set the IP address of an L2TP tunnel peer. This is the peer allowed to establish the tunnel. |
| Local Session ID | Set the numeric identifier for the tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in session establishment message to the L2TP peer. |
| MTU | Define the session MTU as the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data. |
| Remote Session ID | Use the spinner control to set the remote session ID passed in the establishment of the tunnel session. Assign an ID in the range of 1 - 4,294,967,295. |
| Encapsulation | Select either *IP* or *UDP* as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes. |

| | |
|---|---|
| UDP Port | If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. This is the port where the L2TP service is running. |
| Source VLAN | Define the VLAN range (1 - 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames. |
| Native VLAN | Select this option to define the native VLAN that will not be tagged. |

3 Select the **+ Add Row** button in the Cookie table to set the following:

| | |
|---|---|
| Cookie Size | Set the size of the cookie field within each L2TP data packet. Options include 0, 4 and 8. The default setting is 0. |
| Value 1 | Set the cookie value's first word. |
| Value 2 | Set the cookie value's second word. |
| End Point | Define whether the tunnel end point is *local* or *remote.* |

4 Select **OK** to save the changes to the session configuration. Select **Reset** to revert to the last saved configuration.

### *GRE Tunnel Configuration*

GRE tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, access points map one or more VLANs to a tunnel. The remote endpoint is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. access points can reach both the GRE peer as well as the RADIUS server using IPv4.

To define a GRE tunnel configuration:

1 Go to **Configuration → Devices → System Profile** .

The Profile screen displays. This screen lists access point profiles.

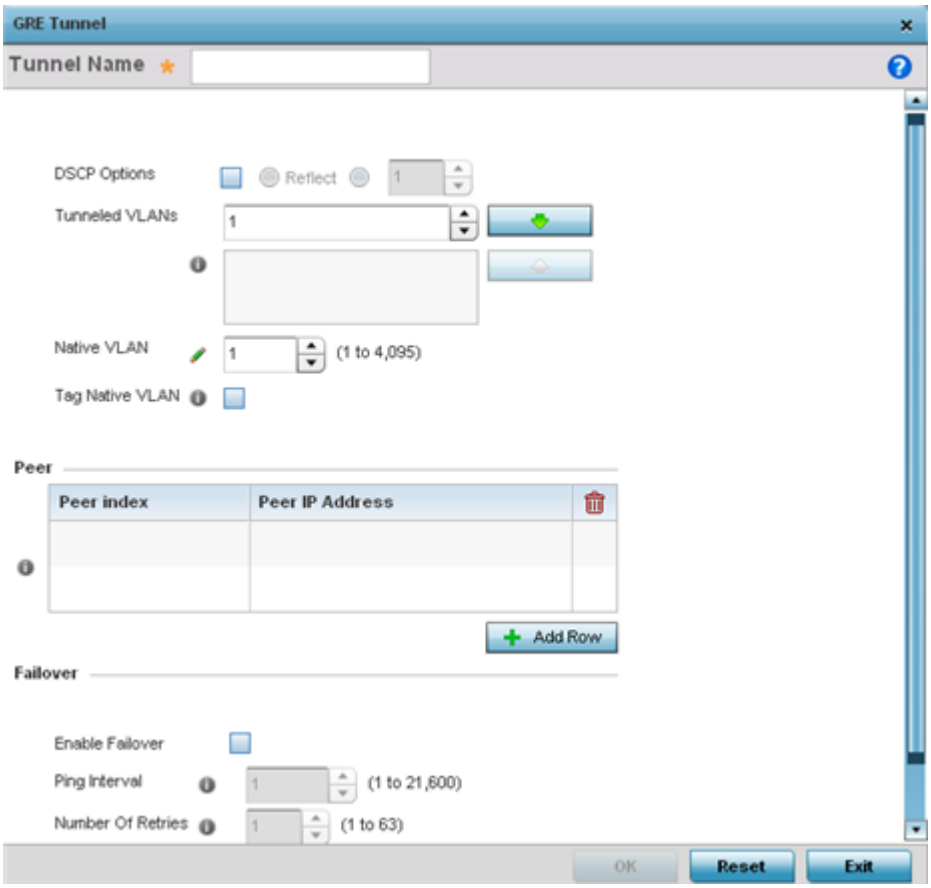
2 Select a profile from the list.

The selected profile's configuration menu displays.

3 Expand the **Network** node and select **GRE**.

The screen displays existing GRE configurations.

4 Select the **Add** to create a new GRE tunnel configuration or select an existing tunnel and select **Edit** to modify its current configuration. To remove an existing GRE tunnel, select it from amongst those displayed and select the **Delete** button.




### Adding and Editing GRE Tunnel

You can add a new GRE tunnel cofiguration or edit an existing tunnel configuration.

1 If creating a new GRE configuration, assign it a name to distinguish its configuration.

2 Define the following GRE tunnel settings:

| | |
|---|---|
| DSCP Options | Use the spinner control to set the tunnel DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header. |
| Tunneled VLANs | Define the VLAN connected clients use to route GRE tunneled traffic within their respective WLANs. |
| Native VLAN | Set a numerical VLAN ID (1 - 4094) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode. |

| | |
|---|---|
| Tag Native VLAN | Select this option to tag the native VLAN. The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default. |
| MTU | Set an IPv4 tunnel's maximum transmission unit (MTU) from 128 - 1,476. The MTU is the largest physical packet size (in bytes) transmittable within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv4, the overhead is 24 bytes (20 bytes IPv4 header + 4 bytes GRE Header), thus the default setting for an IPv4 MTU is 1,476. |
| MTU6 | Set an IPv6 tunnel's MTU from 128 - 1,456. The MTU is the largest physical packet size (in bytes) transmit able within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv6, the overhead is 44 bytes (40 bytes IPv6 header + 4 bytes GRE header), thus the default setting for an IPv6 MTU is 1,456. |

3 In the Peer table, review credentials of existing GRE tunnel end points. If needed, click **+ Add Row** to add new GRE tunnel peers. A maximum of two peer configurations can be added.

| | |
|---|---|
| Peer Index | Assign a numeric index to each peer to help differentiate tunnel end points. |
| Peer IP Address | Define the IP address of the added GRE peer to serve as a network address identifier. |

4 Define the following Failover parameters:

| | |
|---|---|
| Enable Failover | Select this option to periodically ping the primary gateway to assess its availability for failover support. |
| Ping Interval | Set the duration between two successive pings to the gateway. Define this value in seconds from 0 - 86,400. |
| Number of Retries | Set the number of retry ping opportunities before the session is terminated. |

5 Select the **OK** button located to save the changes.

Click **Reset** to revert to the last saved configuration.

### *IGMP Snooping Configuration*

The IGMP *(Internet Group Management Protocol)* is used for managing IP multicast group members. Controllers and service platforms listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the controller or

service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

1 Go to **Configuration → Devices → System Profile** .

The Profile screen displays. This screen lists access point profiles.

2 Select a profile from the list.

The selected profile's configuration menu displays.

3 Expand the **Network** node and select **IGMP Snooping**.

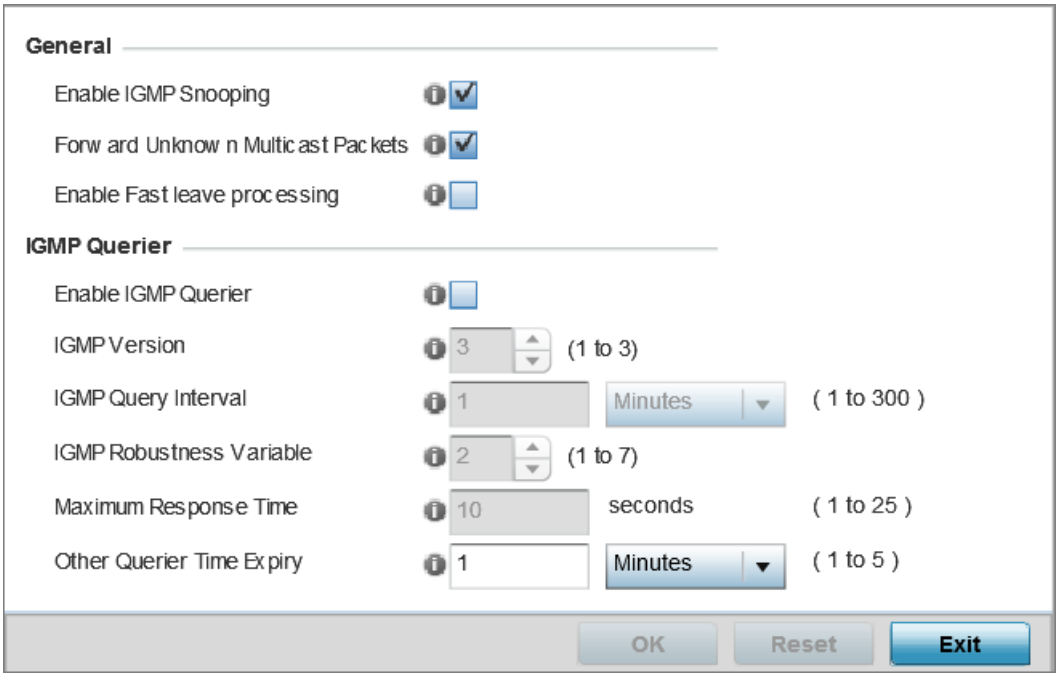



**Figure 49: IGMP Snooping Screen**

4 Set the following parameters to configure General IGMP Snooping values:

| | |
|---|---|
| Enable IGMP Snooping | Select this option to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under the bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the effective setting is disabled. |
| Forward Unknown Multicast Packets | Select this option to enable the forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This setting is enabled by default.. |

5 Set the following IGMP Querier configuration:

| | |
|---|---|
| Enable IGMP Querier | Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server and hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port. |
| IGMP Version | Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 defined by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 by adding the ability to listen to multicast traffic originating from a set of source IP addresses exclusively. The default setting is 3. |
| IGMP Query Interval | Set the interval IGMP queries are made. This parameter is used only when the querier functionality is enabled. Define an interval value in **Seconds** (1 - 18,000), **Minutes** (1 - 300) and **Hours** (1 - 5). The default setting is one minute. |
| IGMP Robustness Variable | Sets the IGMP robustness variable. The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. Define a robustness variable from 1 - 7. The default robustness value is 2. |
| Maximum Response Time | Specify the maximum interval (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. Only multicast packets are forwarded to radios present in the snooping table. For IGMP reports from wired ports, the controller or service platform forwards these reports to the multicast router ports. The default setting is 10 seconds. |
| Other Querier Timer Expiry | Specify an interval in either **Seconds** (60 - 300) or **Minutes** (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute. |

6 Click the **OK** button located at the bottom right of the screen to save the changes.

Click **Reset** to revert to the last saved configuration.

### *MLD Snooping Configuration*

MLD *(Multicast Listener Discovery)* snooping enables a controller, service platform or access point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or access point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To set an IPv6 MLD snooping configuration:

1 Go to **Configuration → Devices → System Profile** .

The Profile screen displays. This screen lists access point profiles.

2 Select a profile from the list.

The selected profile's configuration menu displays.

3 Expand the **Network** node and select **MLD Snooping**.

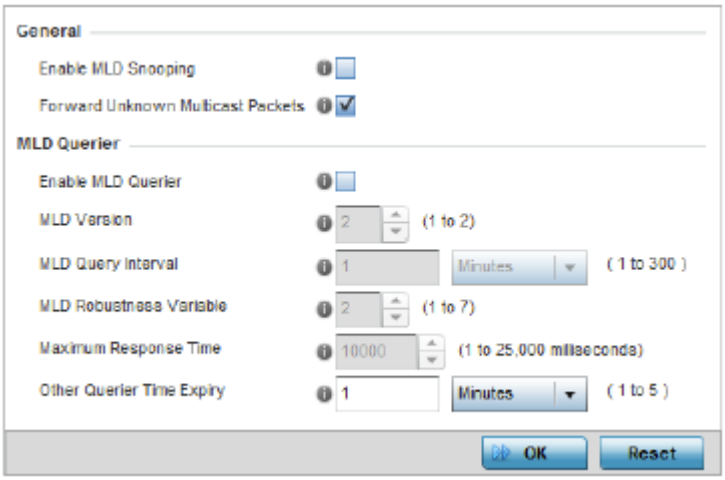



**Figure 50: Profile - Network MLD Snooping screen**

4 Define the following General MLD snooping settings:

| | |
|---|---|
| Enable MLD Snooping | Enable MLD snooping to examine MLD packets and make content forwarding for this profile. Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast. MLD snooping is disabled by default. |
| Forward Unknown Multicast Packets | Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default. |

5 Define the following MLD Querier settings for the MLD snooping configuration:

| | |
|---|---|
| Enable MLD Querier | Select this option to enable MLD querier on the controller, service platform or access point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is disabled by default. |
| MLD Version | Define whether MLD version 1 or 2 is utilized as the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2. |
| MLD Query Interval | Set the interval in which query messages are sent to discover device multicast group memberships. Set an interval in either Seconds (1 -18,000), Minutes (1 - 300) or Hours (1 - 5). The default interval is 1 minute. |
| MLD Robustness Variable | Set a MLD IGMP robustness value (1 - 7) used by the sender of a query. The MLD robustness variable enables refinements to account for expected packet loss on a subnet. Increasing the robust count allows for more packet loss, but increases the leave latency of the subnetwork unless the value is zero. The default variable is 2. |

| | |
|---|---|
| Maximum Response Time | Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 10 milliseconds. |
| Other Querier time Expiry | Specify an interval in either Seconds (60 - 300) or Minutes (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute. |

6 Select the **OK** button located to save the changes.

Click **Reset** to revert to the last saved configuration.

### *QoS Traffic Shaping Basic Configuration*

The WiNG software uses different *Quality of Service* (QoS) screens to define WLAN and device radio QoS configurations. The **System Profiles → Network → QoS facility** is separate from WLAN and radio QoS configurations, and is used to configure the priority of the different DSCP packet types.

QoS values are required to provide service priority to packets. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

The profile QoS screen maps the 6-bit Differentiated Service Code Point (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies a specific per-hop behavior that is applied to a packet.

To define an QoS configuration for DSCP mappings:

1 Go to **Configuration → Devices → System Profile**.

2 Expand **Network** and select **Quality of Service (QoS)**.

The **Traffic Shaping → Basic Configuration** screen displays by default.

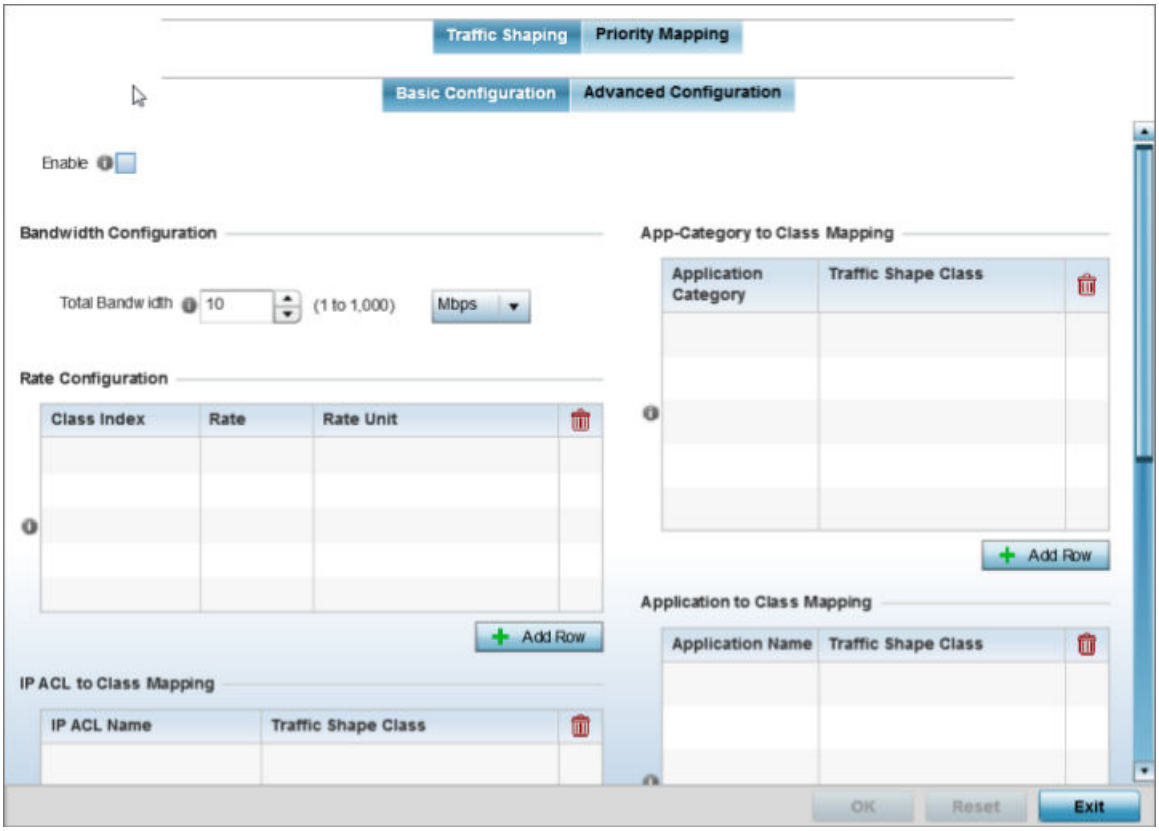



**Figure 51: QoS - Traffic Shaping - Basic Configuration Screen**

3 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, applications have priority, followed by application categories, then ACLs.

4 Set the **Total Bandwidth** configurable for the traffic shaper. Set the value from either 1 - 1,000 Mbps, or from 250 - 1,000,000 Kbps.

5 Select **+ Add Row** within the Rate Configuration table to set the Class Index (1 - 4) and Rate (in either Kbps, Mbps or percentage) for the traffic shaper class. Use the rate configuration to control the maximum traffic rate sent or received on the device. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.

6 Refer to the IP ACL Class Mapping table and select **+ Add Row** to apply an IPv4 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings.

7 Refer to the IPv6 ACL Class Mapping table and select **+ Add Row** to apply an IPv6 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings.

Note

For more information on creating IP based firewall rules, refer to Configuring IP Firewall Rules on page 744 and Setting an IPv4 or IPv6 Firewall Policy on page 745.

8 Refer to the App-Category to Class Mapping table and select + Add Row to apply an application category to shaper class mapping. Select + Add Row to add mappings by selecting the application category and its traffic shaper class. For more information on creating an application category, refer to Application on page 718.

9 Refer to the Application to Class Mapping table and select + Add Row to apply an application to shaper class mapping. Select **+ Add Row** to add mappings by selecting the application and its traffic shaper class. For more information on creating an application, refer to Application on page 718.

10 Select the **OK** button to save the traffic shaping basic configuration changes.

Select **Reset** to revert to the last saved configuration.

### QoS Traffic Shaping Advanced Configuration

To define traffic shaping advanced configuration:

1 Select the Advanced Configuration tab.

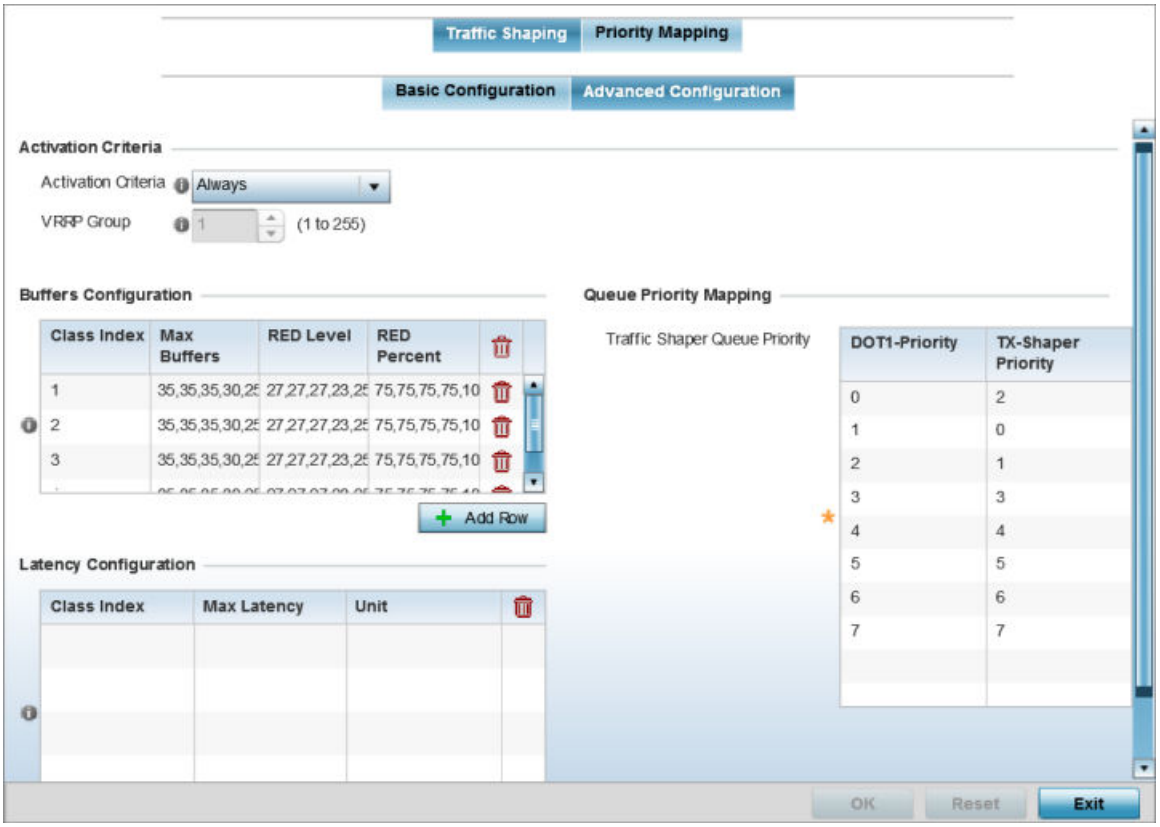



**Figure 52: Profile Overrides - Network QoS Traffic Shaping Advanced Configuration Screen**

2 In the Activation Criteria field, set the following traffic shaper activation criteria:

| | |
|---|---|
| Activation Criteria | Use the drop-down menu to determine when the traffic shaper is invoked. Options include vrrp-master, cluster-master, rf-domain-manager and Always. A VRRP master responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. The solitary cluster master is the cluster member elected, using a priority assignment scheme, to provide management configuration and Smart RF data to other cluster members. Cluster requests go through the elected master before dissemination to other cluster members. The RF Domain manager is the elected member capable of storing and provisioning configuration and firmware images for other members of the RF Domain. |
| VRRP Group | Set the VRRP group ID from 1 - 255. VRRP groups is only enabled when the Establishment Criteria is set to vrrp-master. |

3 Select **+ Add Row** within the Buffers Configuration table to set the following:

| | |
|---|---|
| Class Index | Set a class index from 1 - 4. |
| Max Buffers | Set the Max Buffers to specify the queue length limit after which the queue starts to drop packets. Set the maximum queue lengths for packets. The upper length is 400 for access points. |
| RED Level | Set the packet queue length for RED. The upper limit is 400 for Access Points. The rate limiter uses the RED *(random early detection)* algorithm for rate limiting traffic. RED is a queueing technique for congestion avoidance. RED monitors the average queue size and drops or marks packets. If the buffer is near empty, all incoming packets are accepted. When the queue grows, the probability for dropping an incoming packet also grows. When the buffer is full, the probability has reached 1 and all incoming packets are dropped. |
| RED Percent | Set a percentage (1 - 100) for RED rate limiting at a percentage of maximum buffers. |

4 Select **+ Add Row** within the Latency Configuration table to set the Class Index (1 - 4), Max Latency and latency measurement Unit. Max latency specifies the time limit after which packets start dropping (maximum packet delay in the queue). The maximum number of entries is 8. Select whether msec (default) or usec is unit for latency measurement.

When a new packet arrives it knows how much time to wait in the queue. If a packet takes longer than the latency value, it is dropped. By default latency is not set, so packets remain in queue for long time.

5 Refer to the Queue Priority Mapping table to set the traffic shaper queue priority and specify a particular queue inside a class. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets mark 802.1p markings.

6 Select the **OK** button located to save the changes to the traffic shaping advanced configuration.

Select **Reset** to revert to the last saved configuration.

### QoS Priority Mapping

1 Select the **Priority Mapping** tab.

The **Quality of Service (QoS) → Priority Mapping** screen displays.

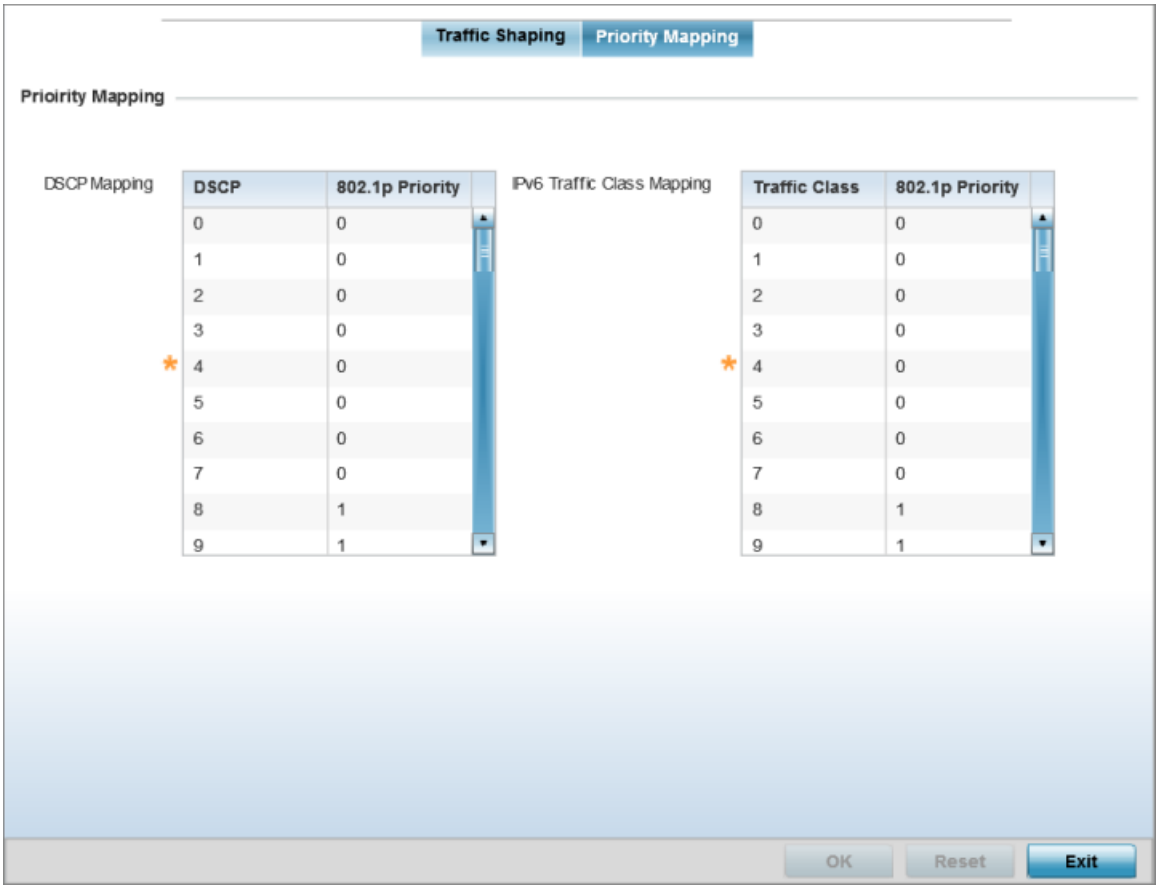



**Figure 53: QoS - Priority Mapping Configuration Screen**

2 In the DSCP Mapping table, set the following IP DSCP mappings for untagged frames:

| | |
|---|---|
| DSCP | Lists the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. |
| 802.1p Priority | Assign a 802.1p priority as a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are:<br>• 0 – *Best Effort*<br>• 1 – *Background*<br>• 2 – *Spare*<br>• 3 – *Excellent Effort*<br>• 4 – *Controlled Load*<br>• 5 – *Video*<br>• 6 – *Voice*<br>• 7 – *Network Control*<br><br>Note:<br>Use the spinner controls within the **802.1p Priority** field for each DSCP row to change its priority value. |

3 In the IPv6 Traffic Class Mapping table, set or override the following IPv6 DSCP settings for untagged frames:

| | |
|---|---|
| Traffic Class | Devices that originate a packet must identify different classes or priorities for IPv6 packets. Devices use the traffic class field in the IPv6 header to set this priority. |
| 802.1p Priority | Assign a 802.1p priority as a 3-bit IPv6 precedence value in the Type of Service field of the IPv6 header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are:<br>• 0 – *Best Effort*<br>• 1 – *Background*<br>• 2 – *Spare*<br>• 3 – *Excellent Effort*<br>• 4 – *Controlled Load*<br>• 5 – *Video*<br>• 6 – *Voice*<br>• 7 – *Network Control* |

4 Select **OK** to save the priority mapping changes.
Select **Reset** to revert to the last saved configuration.

### *Spanning Tree Configuration*

The MSTP *(Multiple Spanning Tree Protocol)* provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there is just one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

A MSTP supported deployment uses multiple MST regions with multiple MSTI *(MST instances)*. Multiple regions and other STP bridges are interconnected using one single CST *(common spanning tree)*. MSTP includes all of its spanning tree information in a single BPDU *(Bridge Protocol Data Unit)* format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To define the spanning tree configuration:

1 Go to **Configuration → Devices → System Profile** .
The Profile screen displays. This screen lists access point profiles.
2 Select a profile from the list.
The selected profile's configuration menu displays.

3 Expand the **Network** node and select **Spanning Tree**.

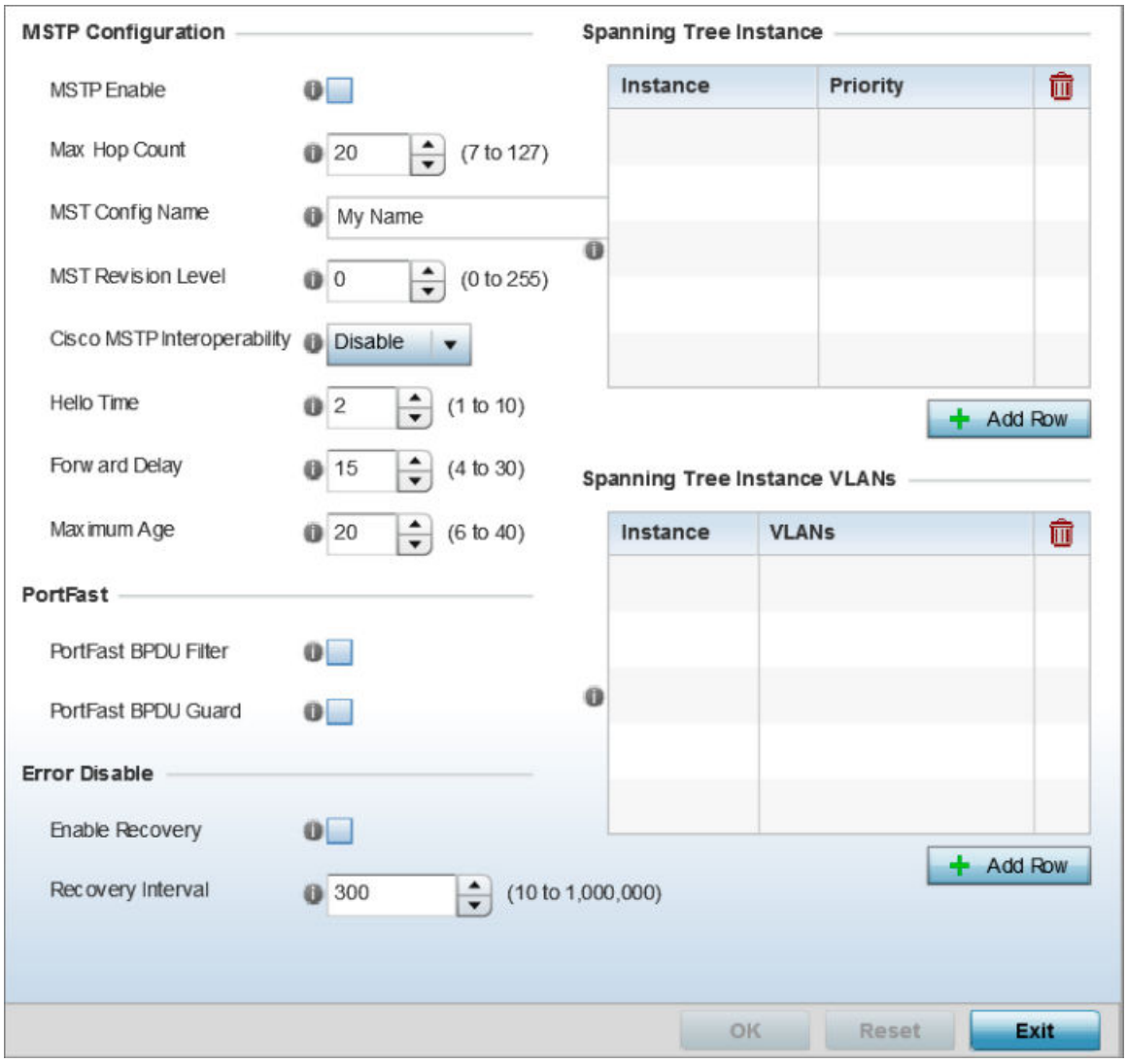



**Figure 54: Network - Spanning Tree Screen**

4 Set the following **MSTP Configuration** parameters:

| | |
|---|---|
| MSTP Enable | Select this option to enable MSTP for this profile. MSTP is disabled by default, so if requiring different (groups) of VLANs with the profile supported network segment. |
| Max Hop Count | Define the maximum number of hops the BPDU will consider valid in the spanning tree topology. The available range is from 7 - 127. The default setting is 20. |
| MST Config Name | Define a 64 character maximum name for the MST region as an identifier. |
| MST Revision Level | Set a numeric revision value ID for MST configuration information. Set a value from 0 - 255. The default setting is 0. |
| Cisco MSTP Interoperability | Select either the Enable or Disable radio buttons to enable/disable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default. |

| | |
|---|---|
| Hello Time | Set a BPDU hello interval from 1 - 10 seconds. BPDUs are exchanged regularly (every 2 seconds by default) and enable supported devices to keep track of network changes and star/stop port forwarding as required. |
| Forward Delay | Set the forward delay time from 4 - 30 seconds. When a device is first attached to a port, it does not immediately start to forward data. It first processes BPDUs and determines the network topology. When a host is attached the port always goes into the forwarding state, after a delay of while it goes through the listening and learning states. The time spent in the listening and learning states is defined by the forward delay (15 seconds by default). |
| Maximum Age | Use the spinner control to set the maximum time (in seconds) to listen for the root bridge. The root bridge is the spanning tree bridge with the smallest (lowest) bridge ID. Each bridge has a unique ID and a configurable priority number, the bridge ID contains both. The available range is from 6 - 40. The default setting is 20. |

5 Define the following **Port Fast** parameters for the profile configuration:

| | |
|---|---|
| PortFast BPDU Filter | Select Enable to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. BPDUs are exchanged regularly and enable the access point to keep track of network changes and to start and stop port forwarding as required. The default setting is disabled. |
| PortFast BPDU Guard | Select Enable to invoke a BPDU guard for the portfast enabled port. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. BPDUs are exchanged regularly and enable the access point to keep track of network changes and to start and stop port forwarding as required. The default setting is disabled. |

6 Define the following Error Disable settings:

| | |
|---|---|
| Enable Recovery | Select this option to enable a error disable timeout resulting from a BPDU guard. This setting is disabled by default. |
| Recovery Internal | Define the recovery interval used to enable disabled ports. The available range is from 10 - 1,000,000 seconds with a default setting of 300. |

7 Use the Spanning Tree Instance table to add indexes to the spanning tree topology.

Add up to 16 indexes and use the Priority setting to define the bridge priority used to determine the root bridge. The lower the setting defined, the greater the likelihood of becoming the root bridge in the spanning tree topology.

8 Use the Spanning Tree Instance VLANs table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.

9 Select the **OK** button located at the bottom right of the screen to save the changes.

Select **Reset** to revert to the last saved configuration.

### *IPv4 Routing Configuration*

Routing is the process of selecting IP paths to send access point managed network traffic. Use the Routing screen to set destination IP and gateway addresses enabling assignment of static IP addresses for requesting clients without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file and reduces the resource space required to maintain address pools.

Both IPv4 and IPv6 routes are separately configurable using their appropriate tabs. For IPv6 networks, routing is the part of IPv6 that provides forwarding between hosts located on separate segments within a larger IPv6 network where IPv6 routers provide packet forwarding for other IPv6 hosts.

To override the access point profile's static routes:

1 Go to **Configuration → Devices → System Profiles**.

2 Expand **Network** and select **Routing**.

The IPv4 Routing configuration screen displays.

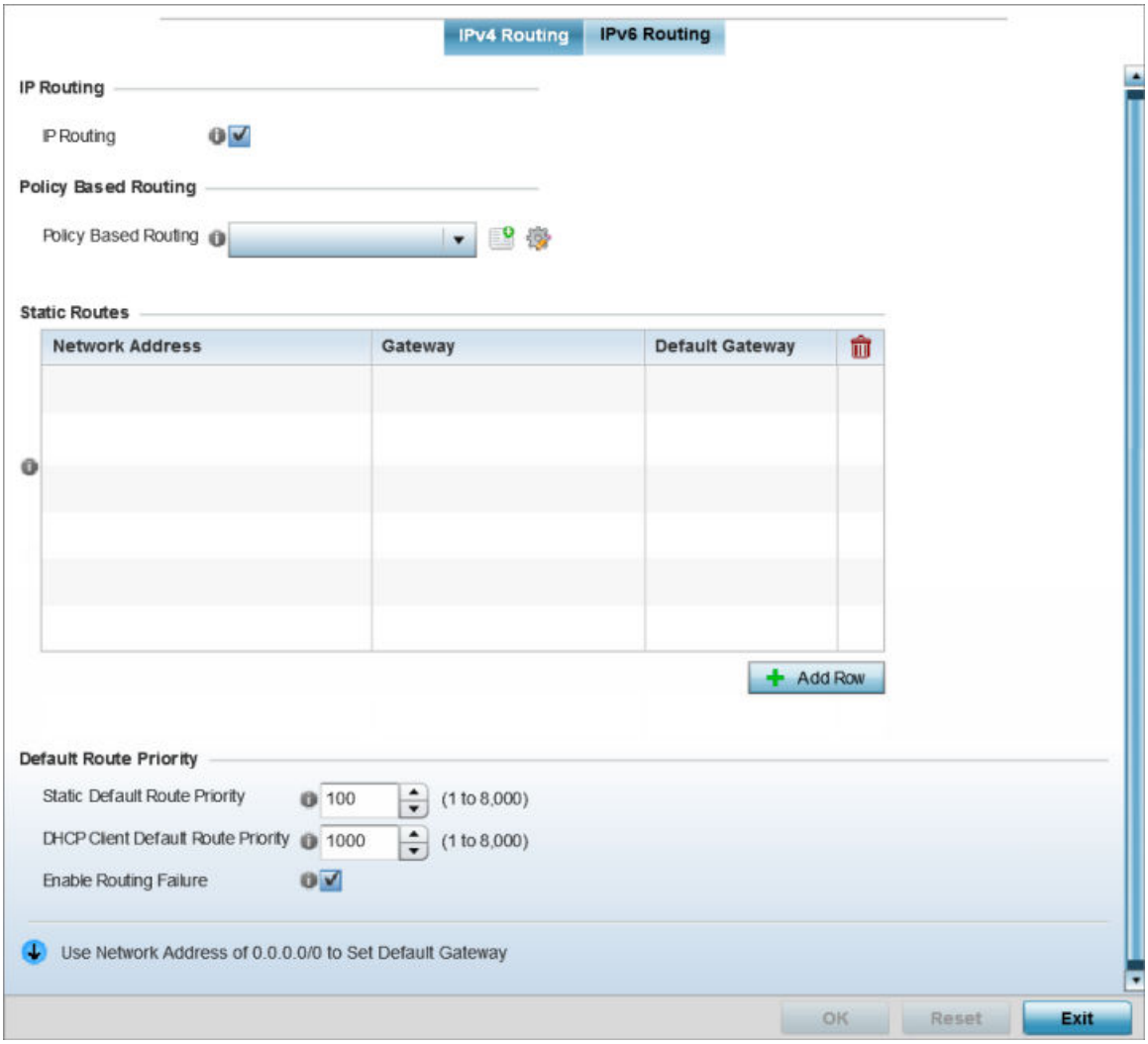



**Figure 55: Profile Overrides - IPv4 Routing Configuration Screen**

3 Select **IP Routing** to enable static routes using IPv4 addresses. This option is enabled by default.

4 In the Policy Based Routing field, use the Policy Based Routing drop-down menu to apply a policy. Select the **Create** icon to create a policy based route or select the **Edit** icon to edit an existing policy after selecting it in the drop-down list. For more information on creating a Policy Based Routing Policy, see Policy Based Routing (PBR) on page 676.

5 in the Statis Routes table, click **Add Row +** and provide the following statis route details:

| | |
|---|---|
| Network Address | Add network IP addresses and network masks |
| Gateway | Provide the Gateway's IP address. This is the gateway used to route traffic to the specified network. |
| Default Gateway | Provide the Default Gateway's IP address. This is the gateway used to route traffic to the specified network. |

6 In the Default Route Priority field, and set the following parameters:

| | |
|---|---|
| Static Default Route Priority | Use the spinner control to set the priority value (1 - 8,000) for the default static route. This is weight assigned to this route versus others that have been defined. The default setting is 100. |
| DHCP Client Default Route Priority | Use the spinner control to set the priority value (1 - 8,000) for the default route learnt from the DHCP client. The default setting is 1000. |
| Enable Routing Failure | When selected, all default gateways are monitored for activity. The system will failover to a live gateway if the current gateway becomes unusable. This feature is enabled by default. |

7 Select the **OK** button to save the IPv4 routing configuration changes.

Select **Reset** to revert to the last saved configuration.

### IPv6 Routing Configuration

1 Select the **IPv6 Routing** tab.

IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.

The IPv6 Routing configuration screen displays.

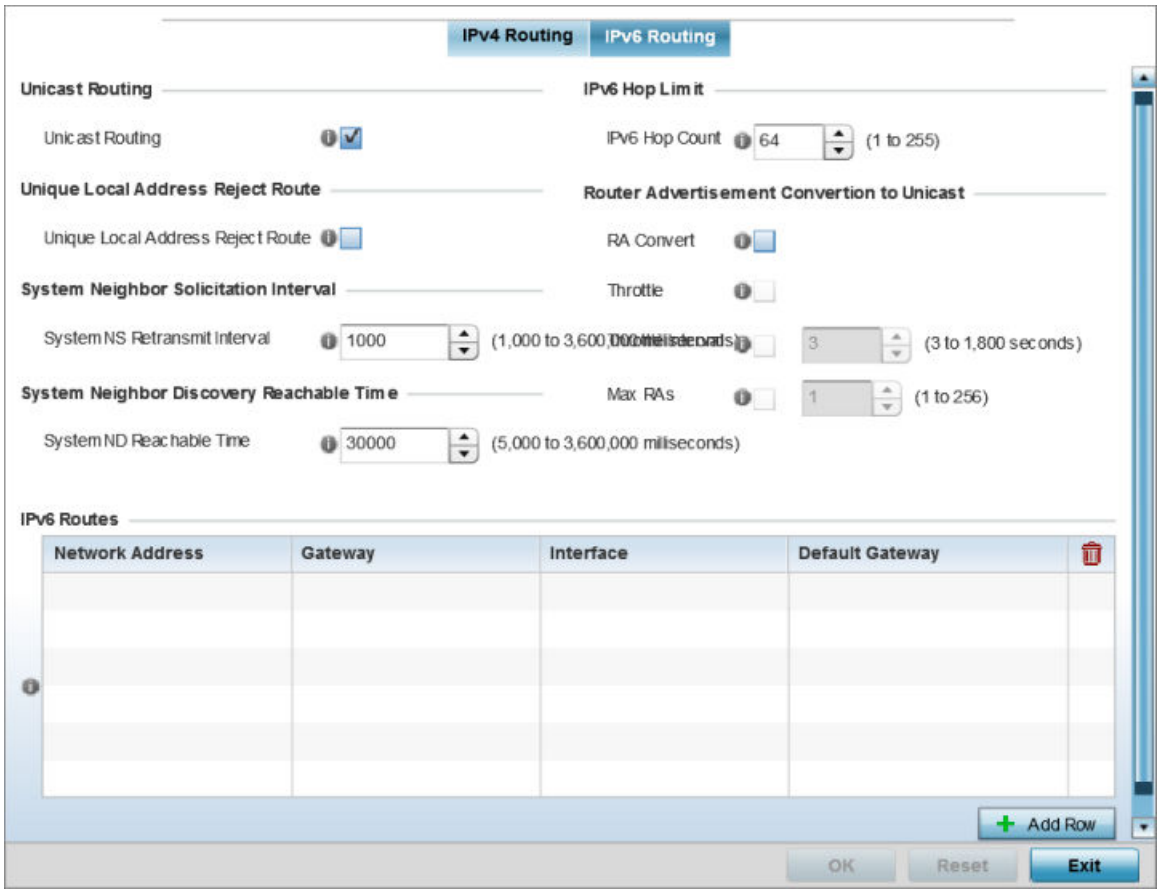



**Figure 56: IPv6 Routing COnfiguration Screen**

2 Select Unicast Routing to enable IPv6 unicast routing for this profile. Keeping unicast enabled allows the profile's neighbor advertisements and solicitations in unicast (as well as multicast) to provide better neighbor discovery. This setting is enabled by default.

3 Select Unique Local Address Reject Route to enable rejecting local routes in the format FC00::/7.

4 Set a System NS Retransmit Interval (from 1,000 to 3,600,000 milliseconds) as the interval between NS *(neighbor solicitation)* messages. NS messages are sent by a node to determine the link layer address of a neighbor, or verify a neighbor is still reachable via a cached link-layer address. The default is 1,000 milliseconds.

5 Set a System ND Reachable Time (from 5,000 to 3,600,000 milliseconds) as the time a neighbor is assumed to be reachable after receiving a receiving a ND *(neighbor discovery)* confirmation for their reachability. The default is 30,000 milliseconds.

6 Set an IPv6 Hop Count (from 1 - 255) as the maximum number of hops considered valid when sending IP packets. The default setting is 64.

7 Set the following **Router Advertisement Conversion to Unicast** settings:

| | |
|---|---|
| RA Convert (milliseconds) | Select this option to convert multicast router advertisements (RA) to unicast router advertisements at the dot11 layer. Unicast addresses identify a single network interface, whereas a multicast address is used by multiple hosts. This setting is disabled by default. |
| Throttle | Select this option to throttle RAs before converting to unicast. Once enabled, set the throttle interval and maximum number of RAs. This setting is disabled by default. |
| Throttle Interval (milliseconds) | Enable this setting to define the throttle interval (3 - 1,800 seconds). The default setting is 3 seconds. |
| Max RAs | Enable this setting to define the maximum number of router advertisements per router (1 - 256) during the throttle interval. The default setting is 1. |

8 In the **IPv6 Routes** table, click **+ Add Row** and add additional 256 IPv6 route resources.

The IPv6 static route **Add Row** screen displays.

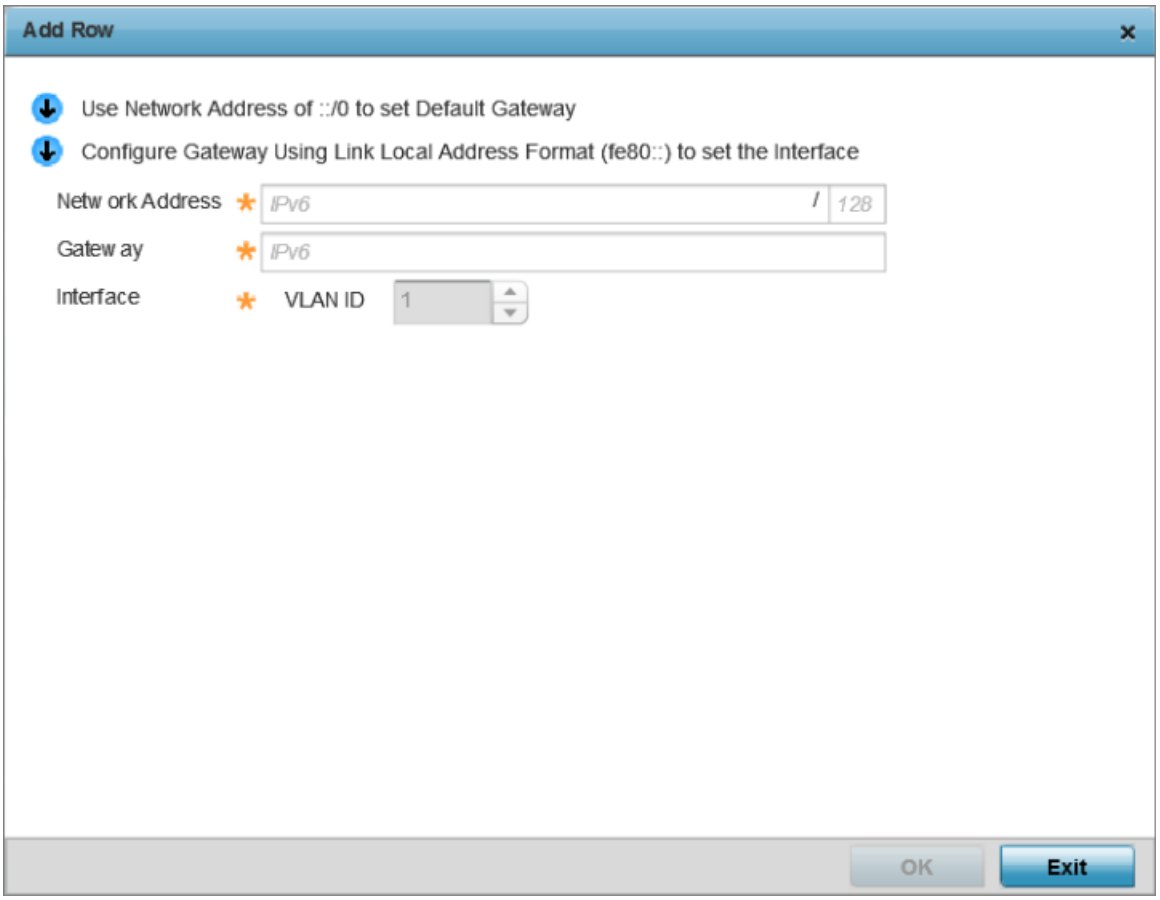



**Figure 57: Add IPv6 Static Route Window**

| | |
|---|---|
| Network Address | Set the IPv6 network address. Other than the length and slightly different look versus an IPv4 address, the IPv6 address concept is same as IPv4. |
| Gateway | Set the IPv6 route gateway. A network gateway in IPv6 is the same as in IPv4. A gateway address designates how traffic is routed out of the current subnet. |
| Interface | If using a link local address, set the VLAN (1 - 4,094) used a virtual routing interface for the local address. |

9 Select **OK** to save the IPv6 static route changes.

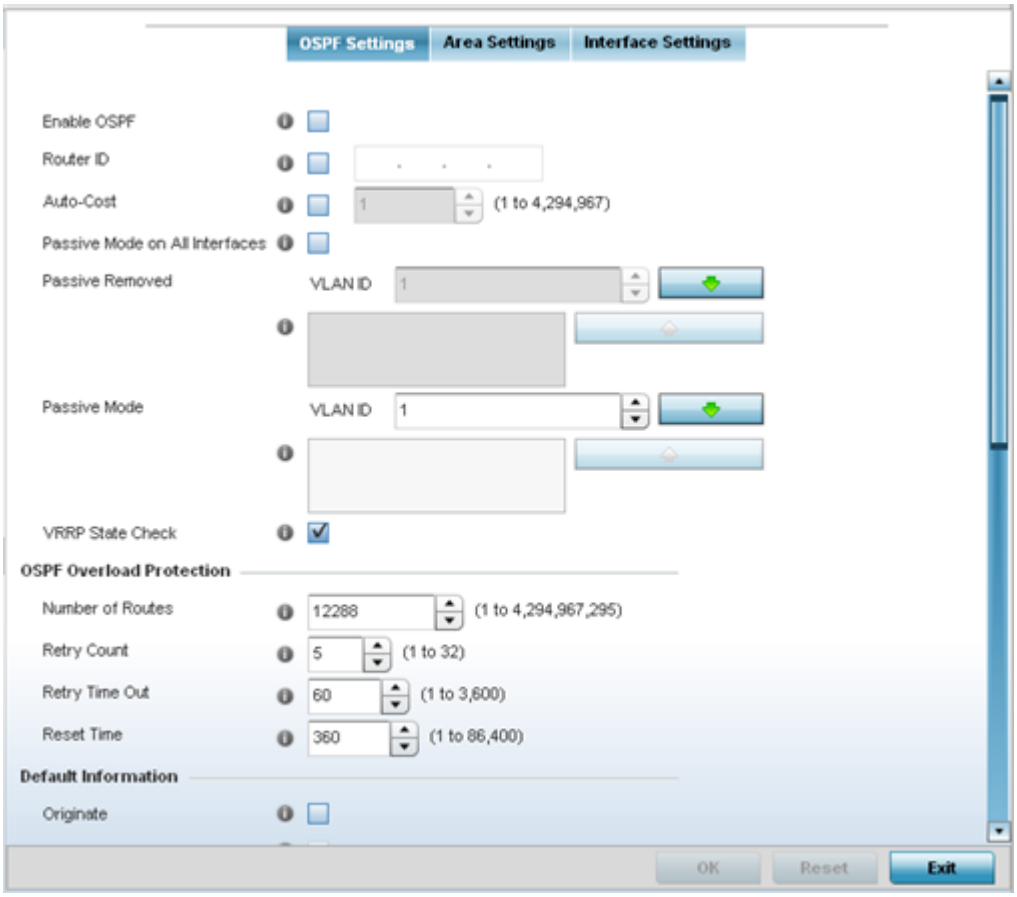
Select **Reset** to revert to the last saved configuration.

*OSPF Settings Configuration*

1 Go to **Configuration → Devices → System Profiles**.

2 Expand **Network** and select **OSPF** .

The OSPF Settings configuration screen displays.




3 Enable/disable OSPF and provide the following dynamic routing settings:

| | |
|---|---|
| Enable OSPF | Select this option to enable OSPF. OSPF is disabled by default. |
| Router ID | Select this option to define a router ID (numeric IP address). This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network. |

| | |
|---|---|
| Auto-Cost | Select this option to specify the reference bandwidth (in Mbps) used to calculate the OSPF interface cost if OSPF is either STUB or NSSA. The default setting is 1. |
| Passive Mode on All Interfaces | When selected, all layer 3 interfaces are set as an OSPF passive interface. This setting is disabled by default. |
| Passive Removed | If *enabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF *non* passive interfaces. Multiple VLANs can be added to the list. |
| Passive Mode | If *disabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF passive interfaces. Multiple VLANs can be added to the list. |
| VRRP State Check | Select this option to use OSPF only if the VRRP interface is not in a backup state. The *Virtual Router Redundancy Protocol* (VRRP) provides automatic assignments of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. This setting is enabled by default. |

4 Set the following OSPF Overload Protection settings:

| | |
|---|---|
| Number of Routes | Use the spinner control to set the maximum number of OSPN routes permitted. The available range is from 1 - 4,294,967,295. |
| Retry Count | Set the maximum number of retries (OSPF resets) permitted before the OSPF process is shut down. The available range is from 1 - 32. The default setting is 5. |
| Retry Time Out | Set the duration (in seconds) the OSPF process remains off before initiating its next retry. The available range is from 1 - 3,600 seconds. The default is 60 seconds. |
| Reset Time | Set the reset time (in seconds) that, when exceeded, changes the retry count is zero. The available range is from 1 - 86,400. The default is 360 seconds. |

5 Set the following Default Information:

| | |
|---|---|
| Originate | Select this option to make the default route a distributed route. This setting is disabled by default. |
| Always | Enabling this setting continuously maintains a default route, even when no routes appear in the routing table. This setting is disabled by default. |
| Metric Type | Select this option to define the exterior metric type (*1* or *2*) used with the default route. |
| Route Metric | Select this option to define route metric used with the default route. OSPF uses path cost as its routing metric. It's defined by the speed (bandwidth) of the interface supporting a given route. |

6 Refer to the Route Redistribution table to set the types of routes that can be used by OSPF.

Select the **+ Add Row** button to populate the table. Set the **Route Type** used to define the redistributed route. Options include *connected*, *kernal* and *static*.

7 Select the **Metric Type** option to define the exterior metric type (1 or 2) used with the route redistribution. Select the Metric option to define route metric used with the redistributed route.

8 Use the OSPF Network table to define networks (IP addresses) to connect using dynamic routes.

Select the **+ Add Row** button to populate the table. Add the IP address and mask of the Network(s) participating in OSPF. Additionally, define the OSPF area (IP address) to which the network belongs.

9 Set an OSPF Default Route Priority (1 - 8,000) as the priority of the default route defined from OSPF.

10 Click **OK** to save the changes made within the screen.

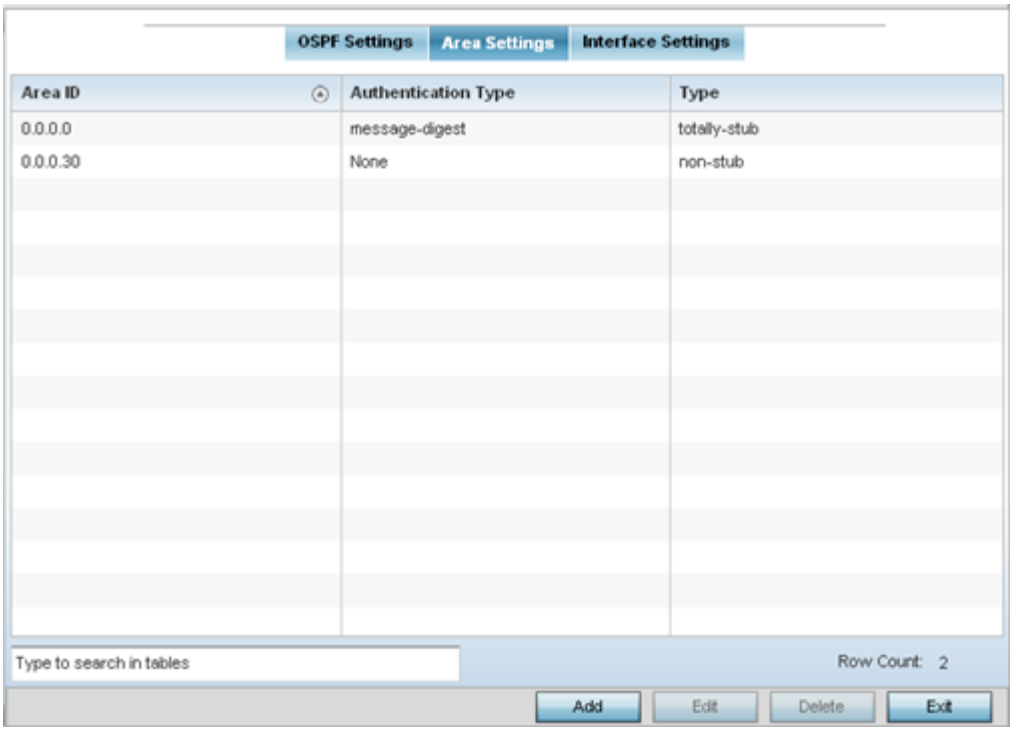
Click **Reset** to revert to the last saved configuration.

### Area Settings

To define a dynamic routing area configuration:

1 Select the **Area Settings** tab.

An OSPF *Area* contains a set of routers exchanging LSAs *(Link State Advertisements)* with others in the same area. Areas limit LSAs and encourage aggregate routes.



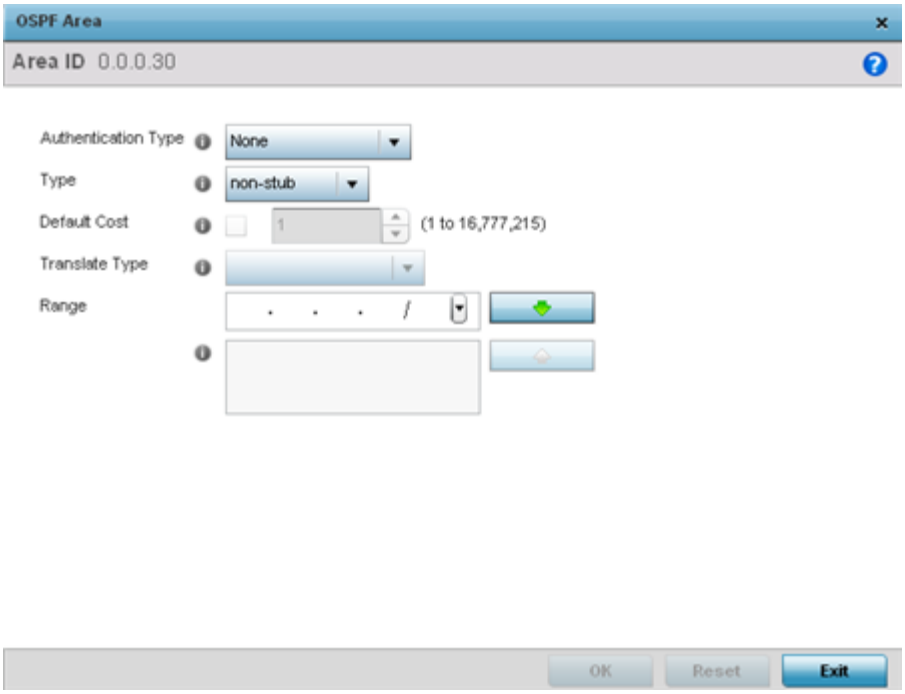

2 Review the following Area Setting configurations to determine if a new configuration needs to be added or existing settings warrants modifications:

| | |
|---|---|
| Area ID | Displays either the *IP address* or *integer* representing the OSPF area. |
| Authentication Type | Lists the authentication (user validation) types used to validate and authenticate the credentials of the dynamic route connections. |
| Type | Lists the OSPF area type in each listed configuration. |

Adding and Editing Area Settings

You can add a new Area configuration or edit an existing configuration.

1 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.




2 Set the following OSPF Area configurations:

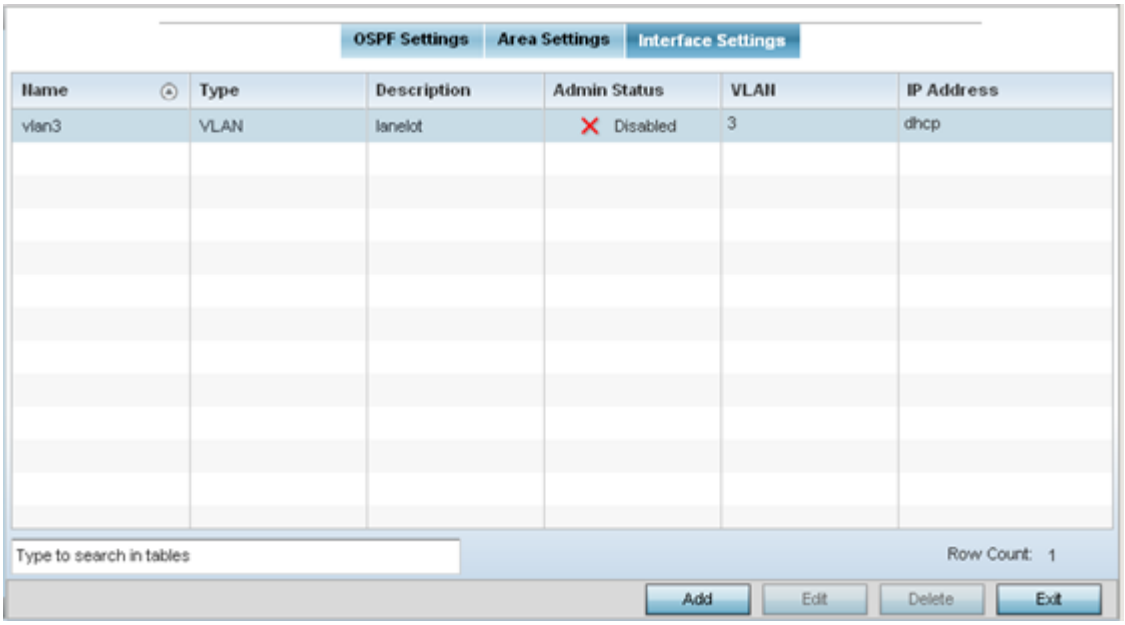
| | |
|---|---|
| Area ID | If adding a new OSPF Area, use the drop-down menu and specify the Area ID either as an *IP address* or *Integer*. |
| Authentication Type | Select either *None*, *simple-password* or *message-digest* as the credential validation scheme used with the OSPF dynamic route. The default setting is None (no data protection). |
| Type | Set the OSPF area type as either *stub*, *totally-stub*, *nssa*, *totally-nssa* or *non-stub*. |
| Default Cost | Select this option to set the default summary cost advertised if creating a stub. Set a value from 1 - 16, 777,215. |
| Translate Type | Define how messages are translated. Options include *translate-candidate*, *translate always* and *translate-never.* The default setting is translate-candidate. |
| Range | Specify a range of addresses for routes matching address/mask for OSPF summarization. |

3 Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

### OSPF Interface Settings

To define a dynamic routing configuration:

1 Select the **Interface Settings** tab.




2 Review existing **Interface Settings** using the following:

| | |
|---|---|
| Name | Displays the name defined for the interface configuration. |
| Type | Displays the type of interface. |
| Description | Lists each interface's 32 character maximum description. |
| Admin Status | Displays whether Admin Status privileges have been *enabled* or *disabled* for the OSPF route's virtual interface connection. |
| VLAN | Lists the VLAN IDs set for each listed OSPF route virtual interface. |
| IP Address | Displays the IP addresses defined as virtual interfaces for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually set. |

3 Select the **Add** button to define a new set of virtual interface basic settings, or **Edit** to update the settings of an existing virtual interface configuration.

Basic General Configuration

To configure the VLAN's basic configurations:

1 Select the **Add** button to define a new set of virtual interface basic settings, or **Edit** to update the settings of an existing virtual interface configuration. The **Basic Configuration** screen displays by default, regardless of a whether a new virtual interface is being created or an existing one is being modified. Select the **General** tab if it is not selected by default.

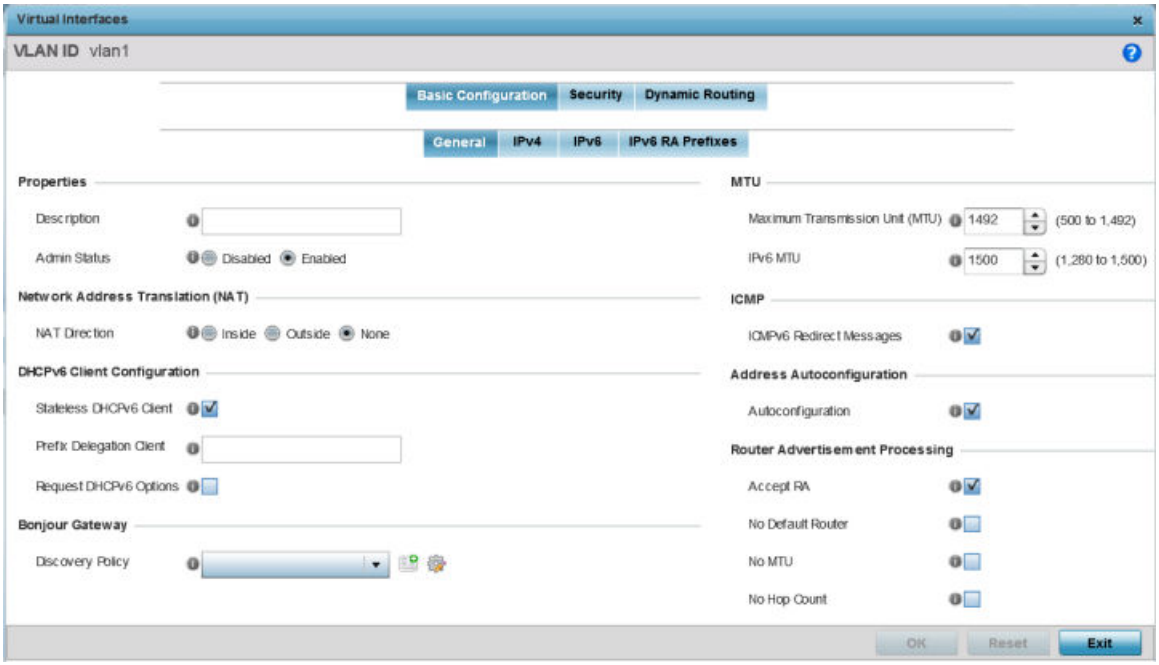



**Figure 58: Profile Overrides - Virtual Interfaces Basic Configuration Screen**

2 If you are creating a new virtual interface, use the **VLAN ID** spinner control to define a numeric VLAN ID from 1 - 4094.

3 Define or override the following parameters in the Properties field:

| | |
|---|---|
| Description | Provide or edit a description (up to 64 characters) for the virtual interface that helps differentiate it from others with similar configurations. |
| Admin Status | Select **Disabled** or **Enabled** to define this interface's current status within the network. When set to **Enabled**, the virtual interface is operational and available. The default value is disabled. |

4 Define or override the Network Address Translation (NAT) direction.

Select one of the following options:

| | |
|---|---|
| Inside | The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. |
| Outside | Packets passing through the NAT on the way back to the managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the switch managed network. |
| None | No NAT activity takes place. This is the default setting. |

5 Set the following DHCPv6 Client Configuration.

The DHCPv6 *(Dynamic Host Configuration Protocol for IPv6)* provides a framework for passing configuration information.

| | |
|---|---|
| Stateless DHCPv6 Client | Select this option to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default. |
| Prefix Delegation Client | Specify a 32-character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface. Devices use prefixes to distinguish destinations that reside on-link from those reachable using a router. |
| Request DHCPv6 Options | Select this option to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than locally. This setting is disabled by default. |

6 Define the Bonjour Gateway settings.

Bonjour is Apple's implementation of zeroconfiguration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers, and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a *local area network* (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

Select the **Bonjour Gateway Discover** policy from the drop-down menu. Click the **Create** icon to define a new Bonjour Gateway policy configuration, or click the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

7 Define the following MTU settings for the virtual interface:

| | |
|---|---|
| Maximum Transmission Unit (MTU) | Set the PPPoE client MTU from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492. |
| IPv6 MTU | Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500. |

8 In the ICMP field, define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route.

This setting is enabled by default.

9 In the Address Autoconfiguration field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits.

This setting is enabled by default.

10 Set the following Router Advertisement Processing settings for the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

| | |
|---|---|
| Accept RA | Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.This setting is enabled by default. |
| No Default Router | Select this option to consider routers unavailable on this interface for default router selection. This setting is disabled by default. |
| No MTU | Select this option to not use the existing MTU setting for router advertisements on this virtual interface. If the value is set to zero, no MTU options are sent. This setting is disabled by default. |
| No Hop Count | Select this option to not use the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default. |

11 Select **OK** to save the changes to the basic configuration. Select **Reset** to revert to the last saved configuration.

Basic IPv4 Configuration

To configure the VLAN IPv4 configuration:

1 Select the **IPv4** tab.

IPv4 is a connectionless protocol. It operates on a best effort delivery model that does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

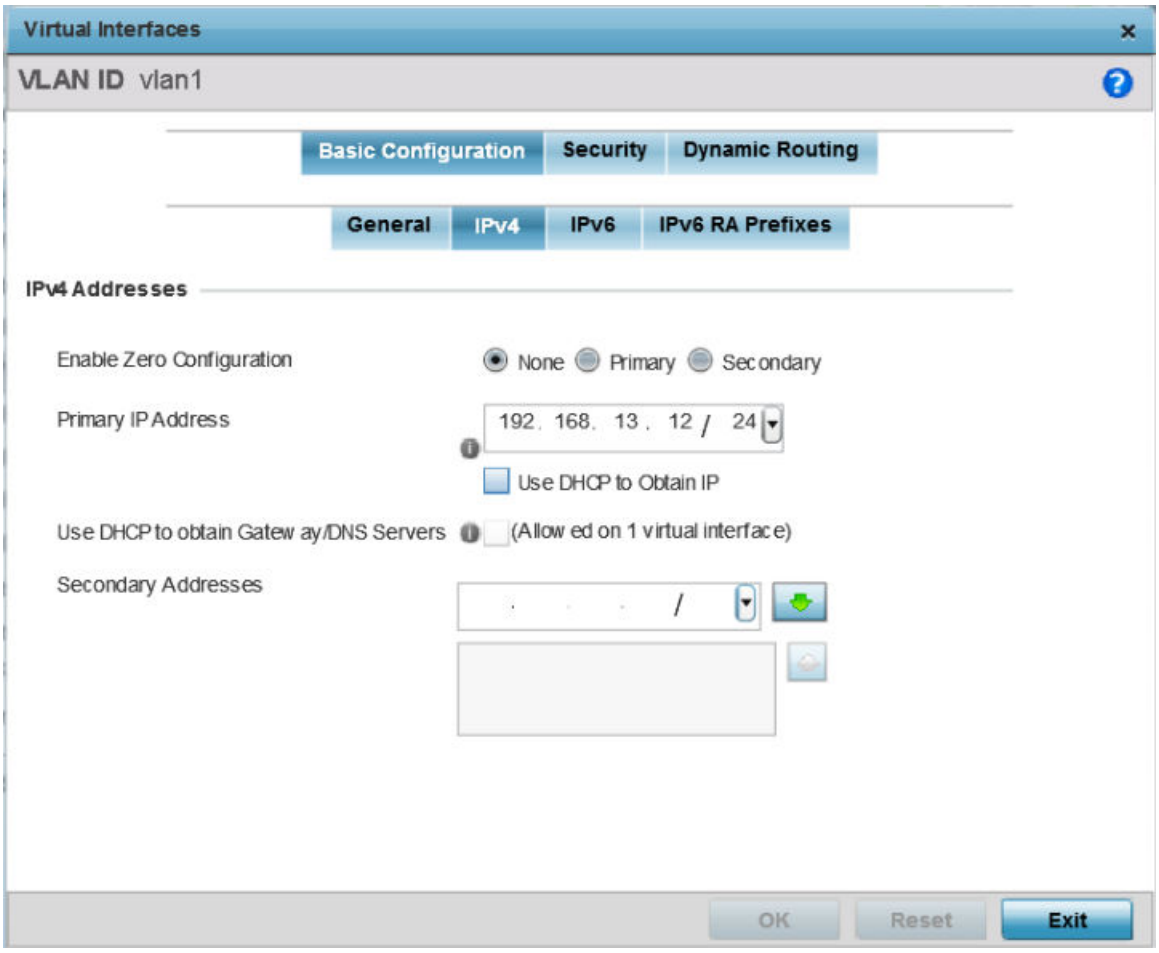



**Figure 59: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv4 Tab**

2 Set the following network information in the IPv4 Addresses field:

| | |
|---|---|
| Enable Zero Configuration | Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to None by default. |
| Primary IP Address | Define the IP address for the VLAN associated virtual interface. |
| Use DHCP to Obtain IP | Select this option to allow DHCP to provide the IP address for the virtual interface. Selecting this option disables the Primary IP Address field. |

| | |
|---|---|
| Use DHCP to Obtain Gateway/DNS Servers | Select this option to allow DHCP to obtain a default gateway address and DNS resource for one virtual interface. This setting is disabled by default and only available when the **Use DHCP to Obtain IP** option is selected. |
| Secondary Addresses | Use this parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable. |

3 Click **OK** to save the changes to the IPv4 configuration.

Click **Reset** to revert to the last saved configuration.

Basic IPv6 Configuration

IPv6 is the latest revision of the IP *(Internet Protocol)*, designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

To configure the VLAN IPv6 configuration:

1 Select the **IPv6** tab.

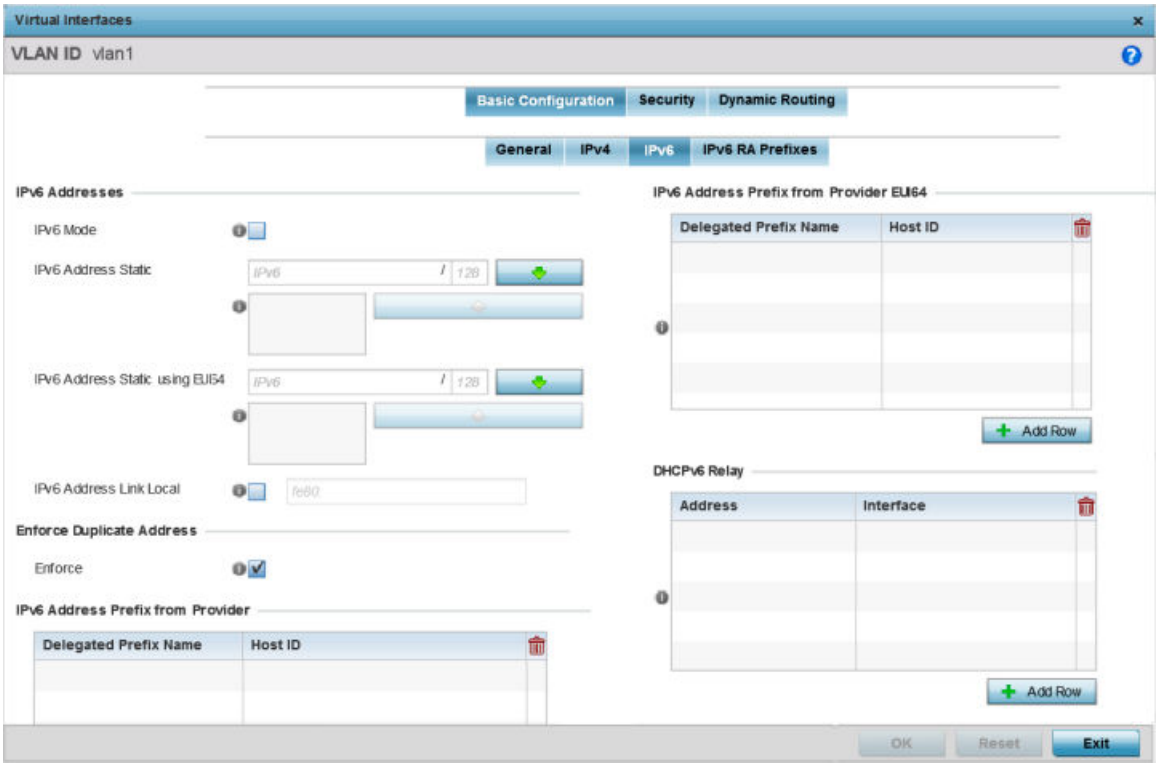



**Figure 60: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab**

2 Refer to the IPv6 Addresses field to define how IP6 addresses are created and utilized:

| | |
|---|---|
| IPv6 Mode | Select this option to enable IPv6 support on this virtual interface. IPv6 is disabled by default. |
| IPv6 Address Static | Define up to 15 global IPv6 IP addresses that can created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons. |
| IPv6 Address Static using EUI64 | Optionally, set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24- bits, with one being an OUI *(Organizationally Unique Identifier)* and the other being client specific. A 16-bit 0xFFFE is then inserted between the two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address. |
| IPv6 Address Link Local | Provide the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled, even when one or more routable addresses are assigned. |

3 Enable the Enforce Duplicate Address option to enforce duplicate address protection when any wired port is connected and in a forwarding state.

This option is enabled by default.

4 Refer to the IPv6 Address Prefix from Provider table to create IPv6 format prefix shortcuts as supplied by an ISP.

Select **+ Add Row** to launch a screen in which a new delegated prefix name and host ID can be defined.

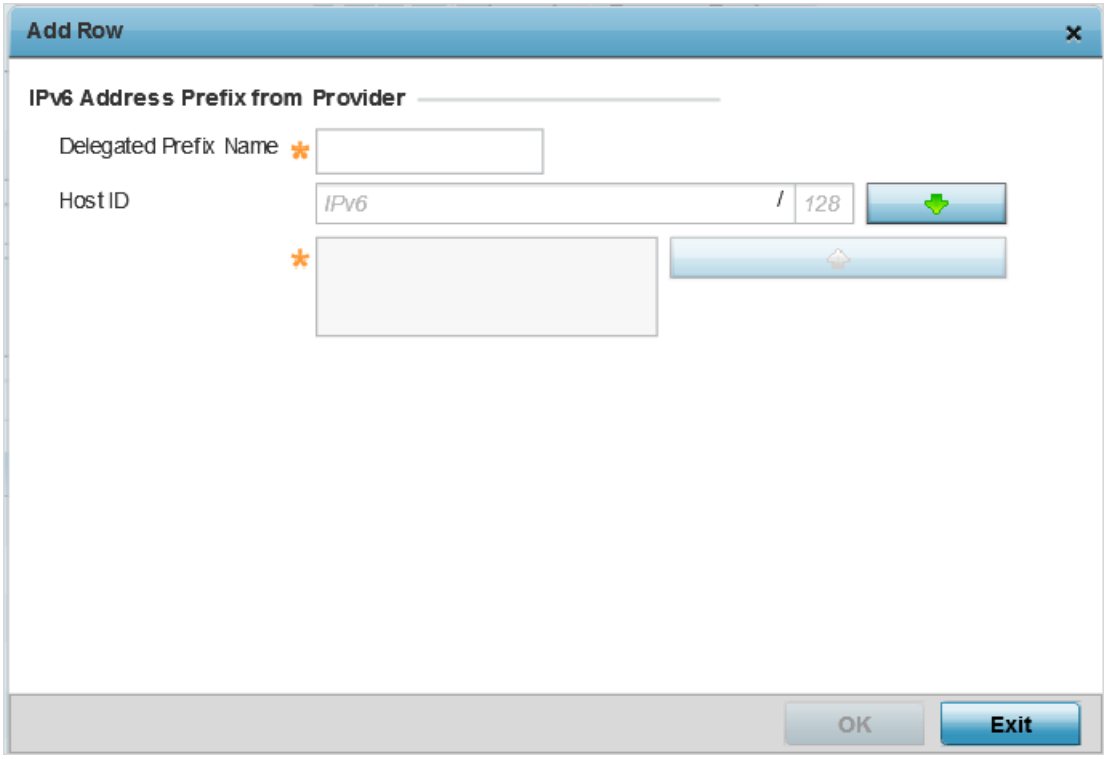



**Figure 61: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider**

| | |
|---|---|
| Designated Prefix Name | Enter a 32-character maximum name for the IPv6 address prefix from your provider. |
| Host ID | Define the subnet ID, host ID, and prefix length. |

5 Click **OK** to save the changes to the IPv6 configuration.

Click **Exit** to close the screen without saving any updates.

6 Refer to the IPv6 Address Prefix from Provider EUI64 table to set an (abbreviated) IP address prefix in EUI64 format.

Select **+ Add Row** to launch a screen in which a new delegated prefix name and host ID can be defined in EUI64 format.

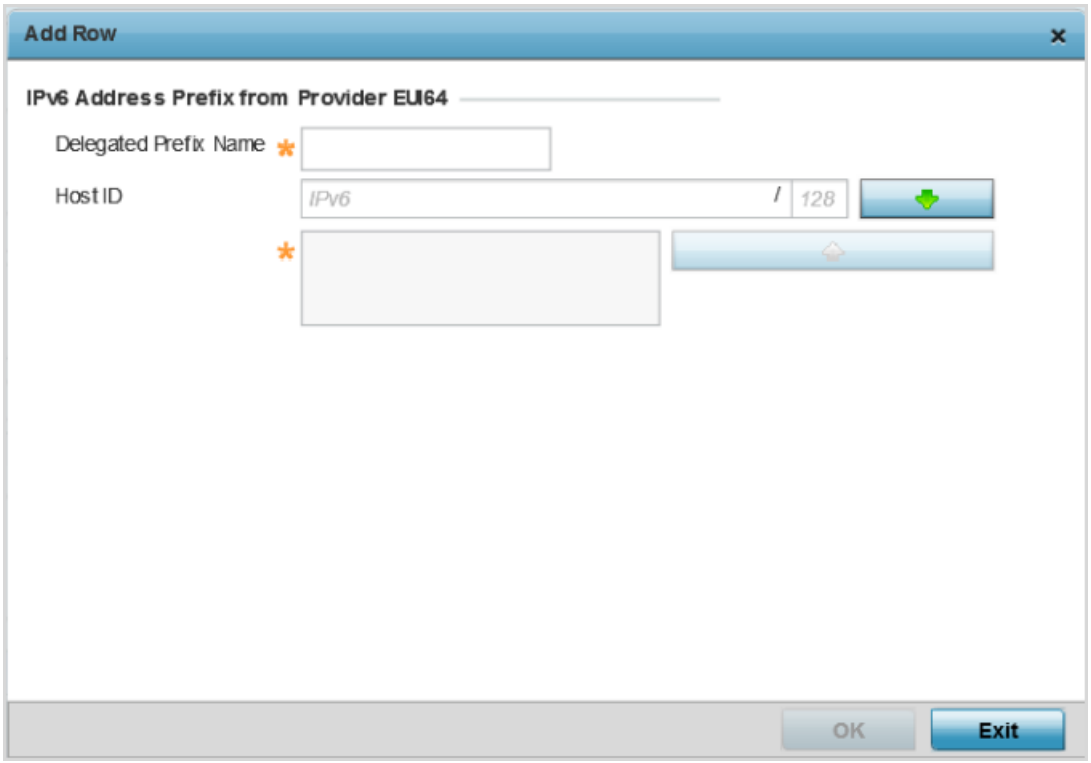



**Figure 62: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider EUI64**

| | |
|---|---|
| Designated Prefix Name | Enter a 32-character maximum name for the IPv6 prefix from your provider in EUI format. Using EUI64, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without manual configuration or DHCP. |
| Host ID | Define the subnet ID and prefix length. |

7 Click **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format.

Click **Exit** to close the screen without saving any updates.

8 Refer to the DHCPv6 Relay table to set the address and interface of the DHCPv6 relay.

The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent

forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

Select **+ Add Row** to launch a screen in which a new DHCPv6 relay address and interface VLAN ID can be set.

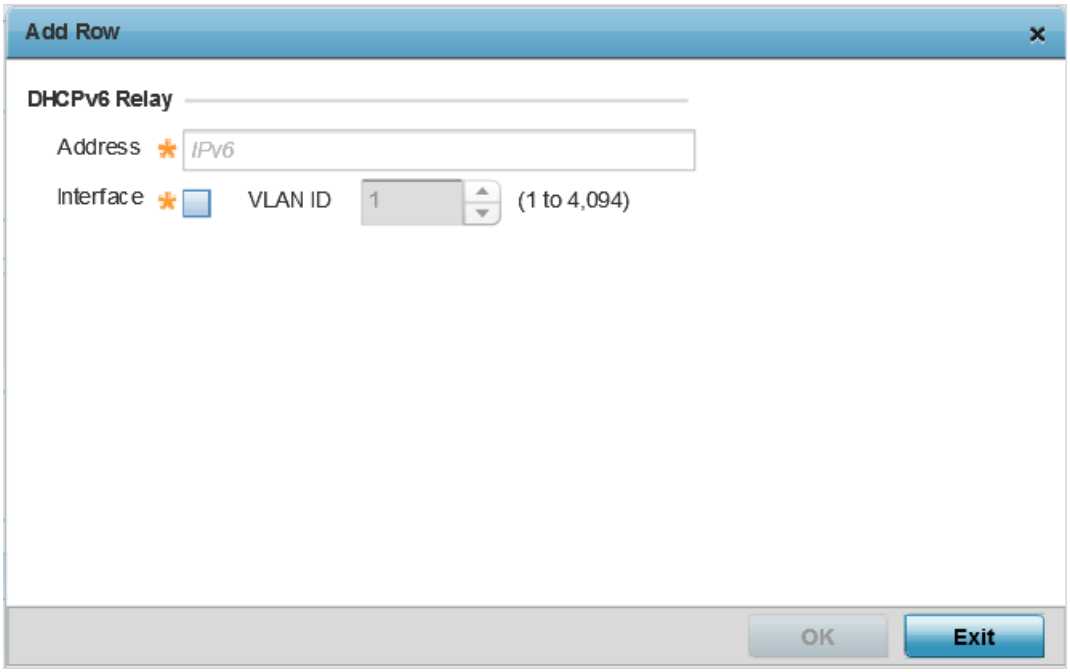



**Figure 63: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add DHCPv6 Relay**

| | |
|---|---|
| Address | Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network. |
| Interface | Select this option to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available. |

9 Click **OK** to save the changes to the DHCPv6 relay configuration.

Click **Exit** to close the screen without saving any updates.

IPV6 Prefix RA Configuration

To configure the VLAN IPv6 RA Prefixes configuration:

1 Select the **IPv6 RA Prefixes** tab.

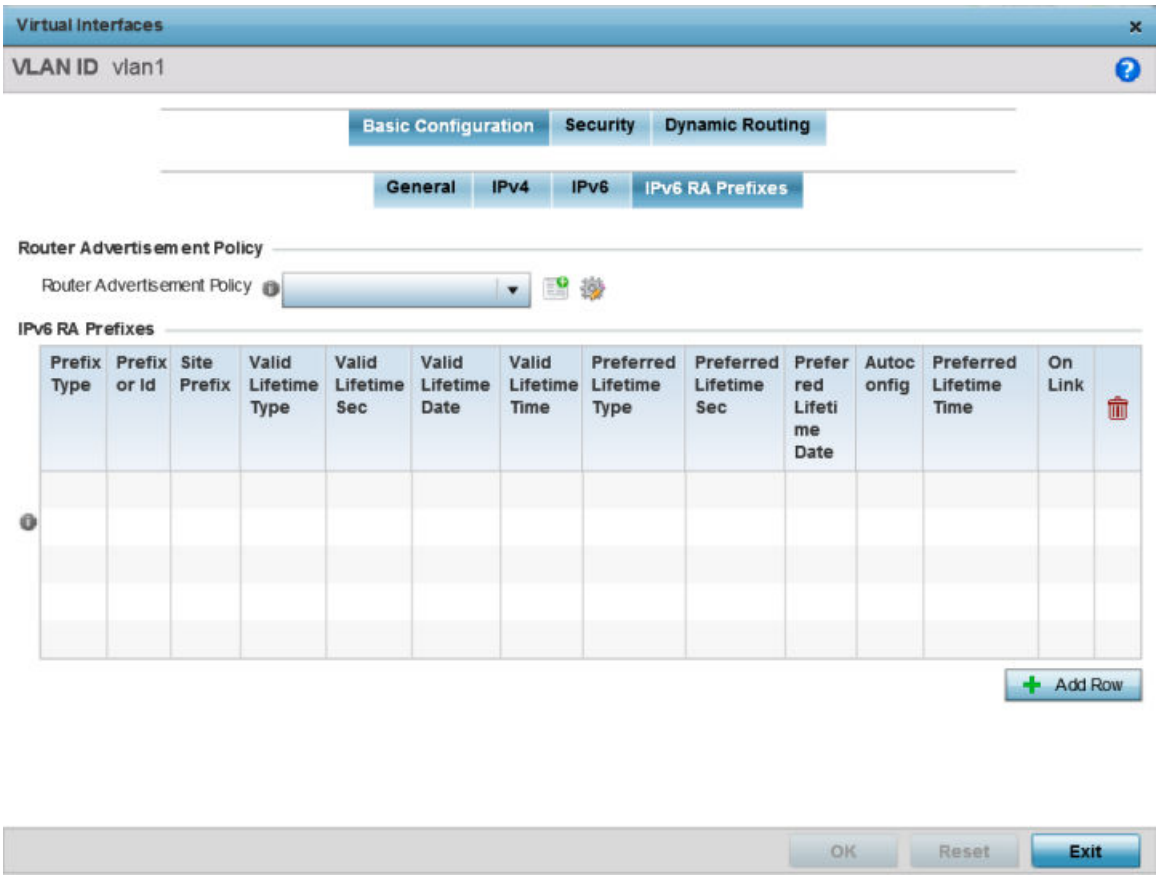



**Figure 64: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefixes Tab**

2 Use the **Router Advertisement Policy** drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

3 Review the configurations of existing IPv6 advertisement policies.

If necessary, select **+ Add Row** to define the configuration for an additional IPv6 RA prefix.

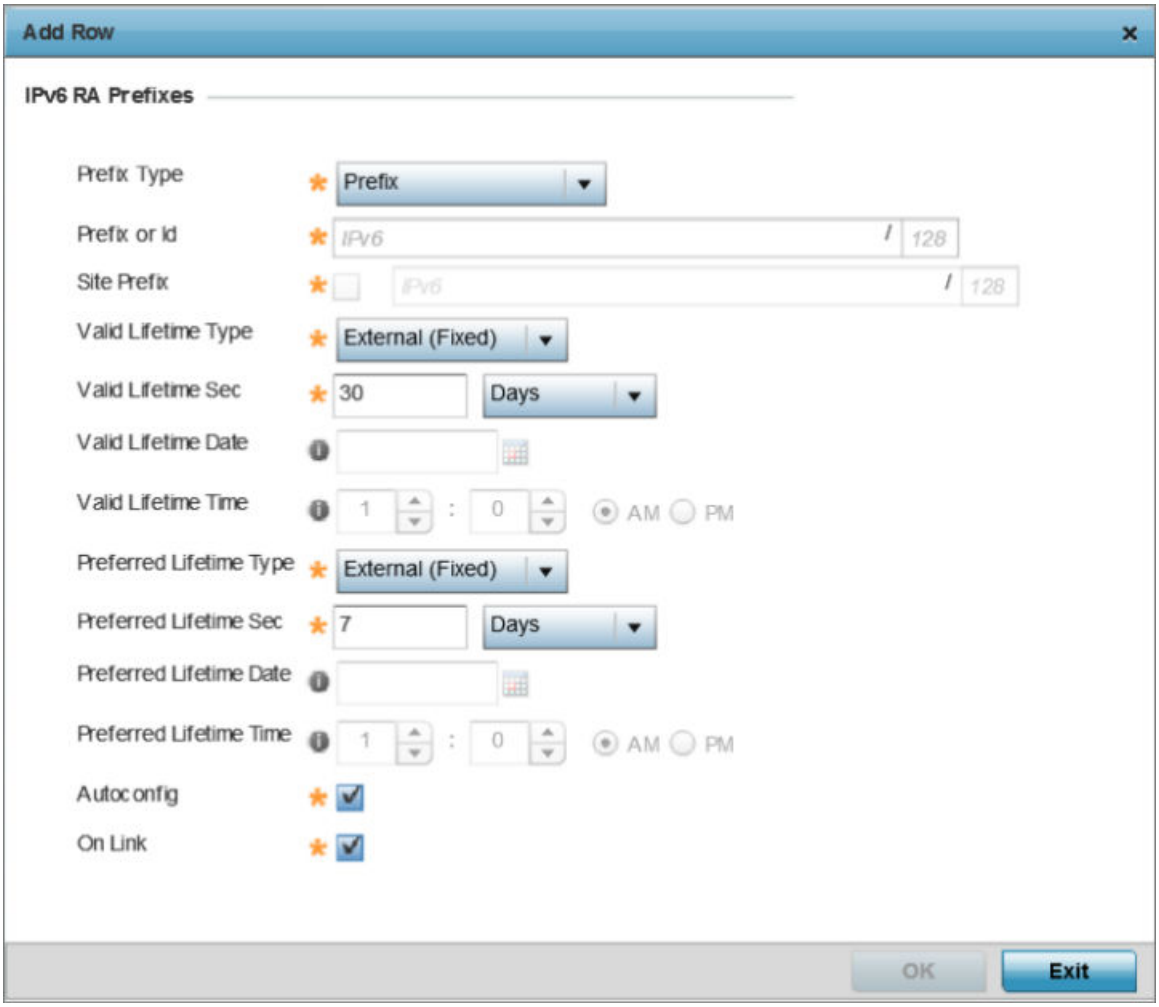



**Figure 65: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefix**

4 Define the following IPv6 RA Prefix settings:

| | |
|---|---|
| Prefix Type | Set the prefix delegation type used with this configuration. Options include **`Prefix`**, and **`prefix-from-provider`**. The default setting is **`Prefix`**. A prefix allows an administrator to associate a user defined name to an IPv6 prefix. A provider assigned prefix is made available from an ISP *(Internet Service Provider)* to automate the process of providing and informing the prefixes used. |
| Prefix or ID | Set the actual prefix or ID used with the IPv6 router advertisement. |
| Site Prefix | The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link. |

| | |
|---|---|
| Valid Lifetime Type | Set the lifetime for the prefix's validity. Options include **External** (fixed), **decrementing,** and **infinite**. If set to **External** (fixed), only the **Valid Lifetime Sec** setting is enabled to define the exact time interval for prefix validity. If set to **decrementing,**, use the lifetime date and time settings to refine the prefix expiry period. If set to **infinite**, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is **External** (fixed). |
| Valid Lifetime Sec | If the lifetime type is set to **External** (fixed), set the Seconds, Minutes, Hours, or Days values used to measure the prefix's expiration. 30 days, 0 hours, 0 minutes, and 0 seconds is the default lifetime. |
| Valid Lifetime Date | If the lifetime type is set to **External** (fixed), set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Valid Lifetime Time | If the lifetime type is set to **decrementing**, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the **AM** and **PM** radio buttons to set the appropriate hour. |
| Preferred Lifetime Type | Set the administrator preferred lifetime for the prefix's validity. Options include **External** (fixed), **decrementing,** and **infinite**. If set to **External** (fixed), only the **Preferred Lifetime Sec** setting is enabled to define the exact time interval for prefix validity. If set to **decrementing,**, use the lifetime date and time settings to refine the prefix expiry period. If set to **infinite**, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is **External** (fixed). |
| Preferred Lifetime Sec | If the administrator preferred lifetime type is set to **External** (fixed), set the Seconds, Minutes, Hours, or Days values used to measure the prefix's expiration. 30 days, 0 hours, 0 minutes, and 0 seconds is the default lifetime. |
| Preferred Lifetime Date | If the administrator preferred lifetime type is set to **External** (fixed), set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Preferred Lifetime Time | If the administrator preferred lifetime type is set to **decrementing**, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the **AM** and **PM** radio buttons to set the appropriate hour. |
| Autoconfig | Autoconfiguration includes generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default. |
| On Link | Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled. |

5 Click **OK** to save the changes to the IPv6 RA prefix configuration.

Click **Exit** to close the screen without saving any updates. Or, click **Reset** to revert to the last saved configuration.

Security

To define a dynamic routing configuration:

1 Select **Configuration → Profiles → System Profile**.

A list of device profiles within the system is displayed.

2 Expand the **Network** menu and select **OSPF**.

3 Select the **Add** button to define a new set of virtual interface basic settings, or **Edit** to update the settings of an existing virtual interface configuration.

4 Select the **Security** tab.

The VLAN Interface security configuration screen displays.

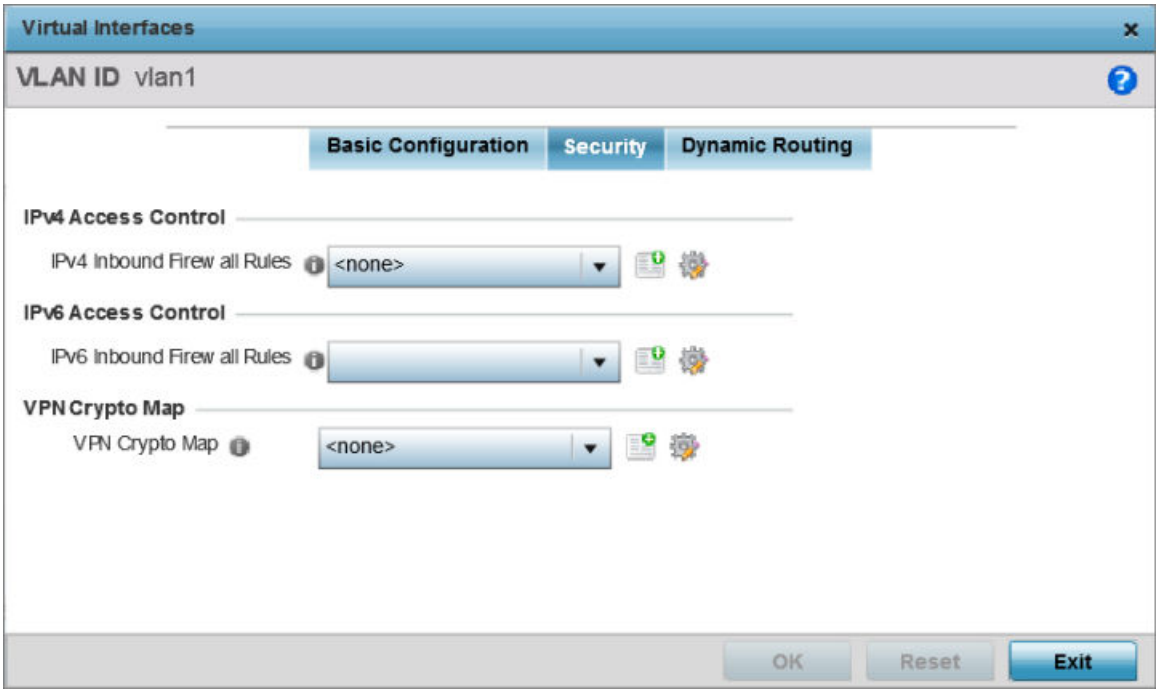



**Figure 66: OSPF - VLAN Interface Security Configuration Screen**

5 Use the **IPv4 Inbound Firewall Rules** drop-down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv4 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

6 Use the **IPv6 Inbound Firewall Rules** drop-down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv6 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

7 Use the **VPN Crypto Map** drop-down menu to select and apply a VPN crypto map entry to apply to the OSPF dynamic route.

Crypto Map entries are sets of configuration parameters for encrypting packets passing through the VPN Tunnel. If a Crypto Map configuration does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new Crypto Map configuration or the **Edit** icon to modify an existing configuration.

8 Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

Dynamic Routing

To define a dynamic routing configuration:

1 Select the **Dynamic Routing** tab.

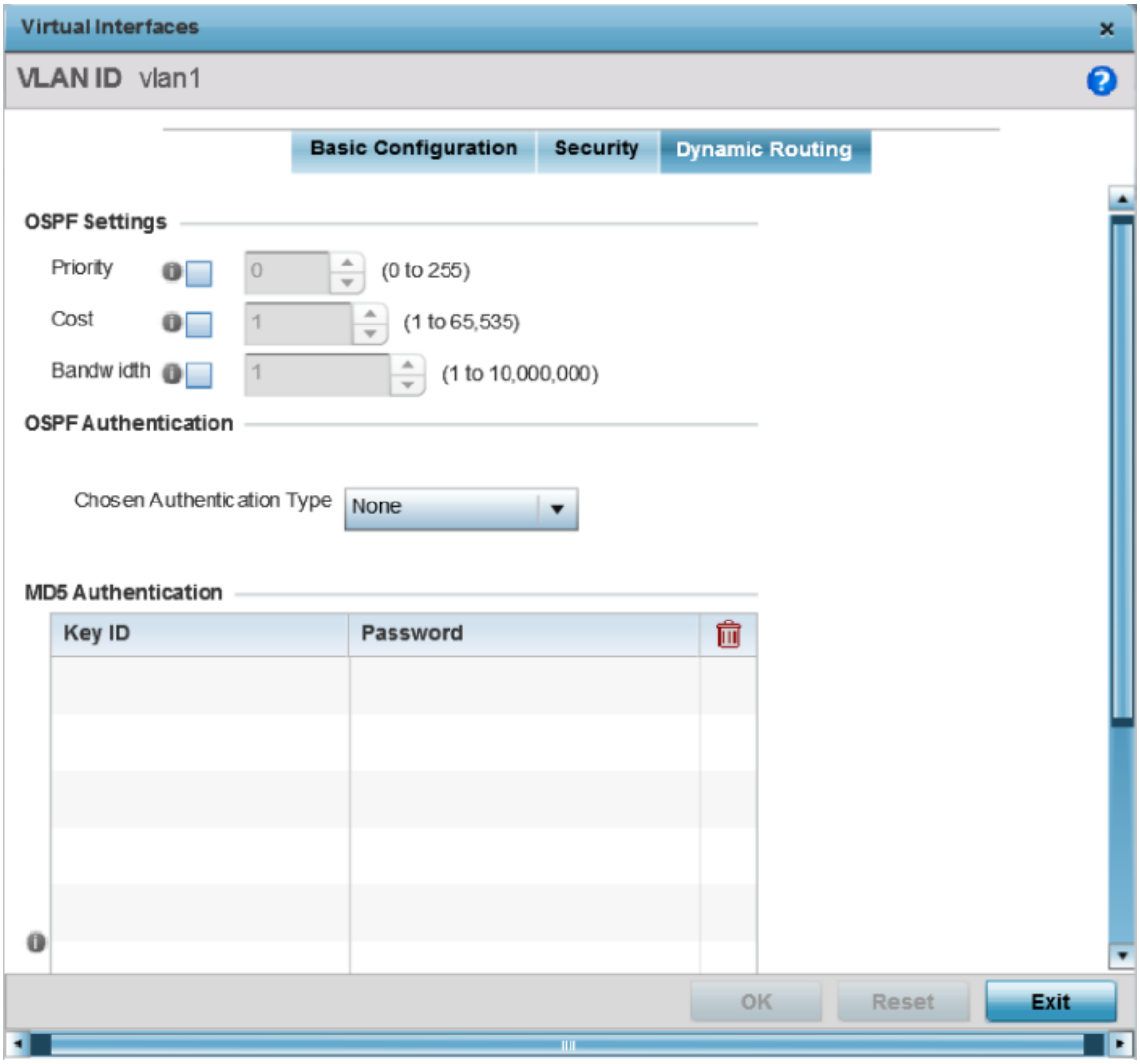



**Figure 67: Profiles OSPF Virtual Interface Dynamic Routing Screen**

2 Set the following OSPF Settings:

| | |
|---|---|
| Priority | Select this option to enable or disable OSPF priority settings. Use the spinner to configure a value from 0 - 255. This option sets the priority of this interface becoming the Designated Router (DR) for the network. DRs provide routing updates to the network by maintaining a complete topology table of the network and sends the updates to the other routers in the network using multicast. Setting a high value increases the chance of this interface becoming a DR. Setting this value to zero prevents this interface from being elected a DR. |
| Cost | Select this option to enable or disable OSPF cost settings. Use the spinner to configure a cost value from 1 - 65535. Use this option to set the OSPF cost of this interface. OSPF cost is the overhead required to send a packet over this interface. |
| Bandwidth | Set the OSPF bandwidth from 1 - 10,000,000 KBps. |

3 Set the following OSPF Authentication settings for the dynamic route:

| | |
|---|---|
| Chosen Authentication Type | Select the authentication type used to validate credentials within the OSPF dynamic route. Options include *simple-password*, *message-digest*, *null* and *None*. |
| Authentication Key | Enter and confirm the authentication key required by connecting nodes using the OSPF dynamic route. |

4 Select the **+ Add Row**w button (at the bottom of the MD5 Authentication table) to add the Key ID and Password used for an MD5 validation of authenticator credentials.

Use the spinner control to set the OSPF message digest authentication key ID. The available range is from 1 - 255. The password is the OSPF key either displayed as series or asterisks or in plain text (by selecting Show).

5 Select **OK** to save the changes to the configuration. Select **Reset** to revert to the last saved configuration

### *Forwarding Database Configuration*

An Forwarding Database forwards or filter packets on behalf of the managing controller, service platform or access point. The bridge reads the packet's destination MAC address and decides to either forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network segment, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to decide to filter or forward the packet.

To define a forwarding database configuration:

1 Select the **Configuration → Devices → System Profile** tab from the Web UI.

2 Expand the **Network** menu and select **Forwarding Database**.

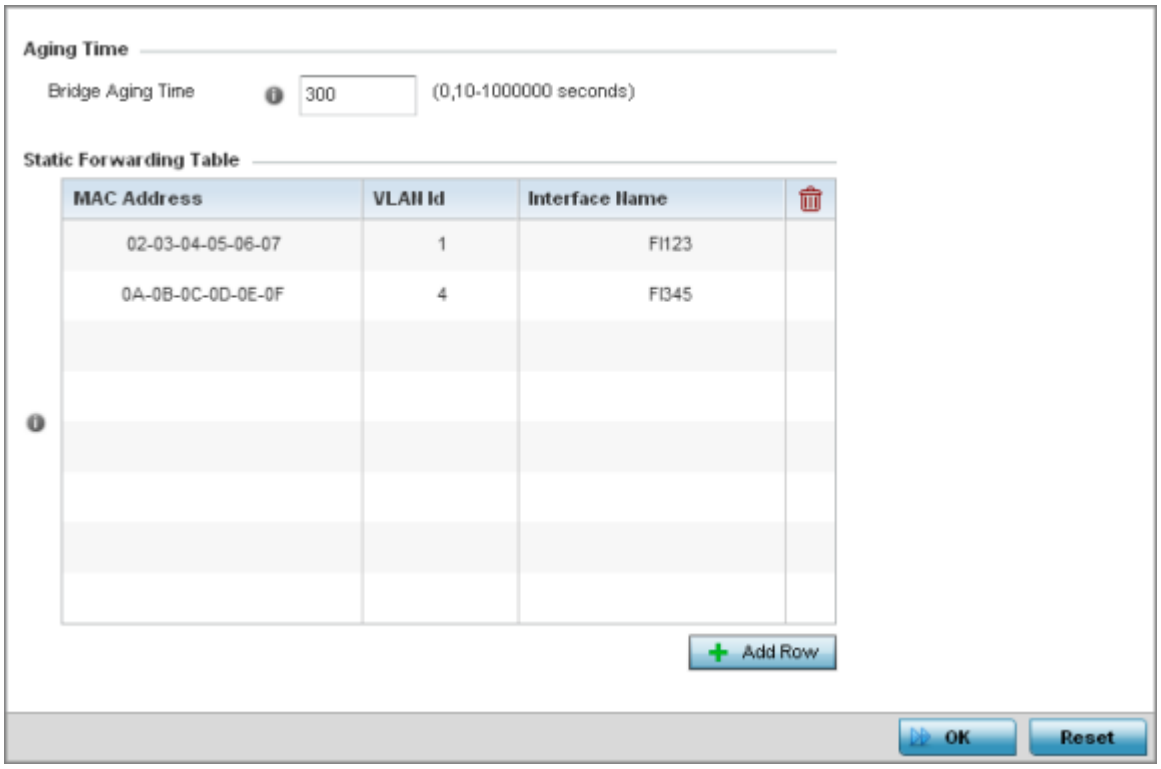



**Figure 68: Network - Forwarding Database screen**

3 Define the **Bridge Aging Time** from 0, 10-1,000,000 seconds.

The aging time defines the length of time an entry will remain in the bridge's forwarding table before it is deleted due to lack of activity. If an entry replenishments a destination, generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table. The default setting is 300 seconds.

4 Use the **+Add Row** button to create a new row within the Static Forwarding Table.

5 Set or override a destination **MAC Address**.

The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered).

6 Define the target **VLAN ID** if the destination MAC is on a different network segment.

7 Provide an **Interface Name** used as the target destination interface for the target MAC address.

8 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

*Bridge VLAN Configuration*

A VLAN is separately administrated virtual network within the same physical managed network. VLANs are broadcast domains defined to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

For example, say several computers are used in conference room X and some in conference Y. The systems in conference room X can communicate with one another, but not with the systems in conference room Y. The creation of a VLAN enables the systems in conference rooms X and Y to communicate with one another even though they are on separate physical subnets. The systems in conference rooms X and Y are managed by the same single device, but ignore the systems that aren't using same VLAN ID.

Administrators often need to route traffic to interoperate between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the Bridge VLAN forwards the data frame on the appropriate port(s). VLAN's are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Controllers and service platforms can do this on their own, without the need to know what VLAN it's on (this is called port-based VLAN, since it's assigned by port). Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security or service quality.

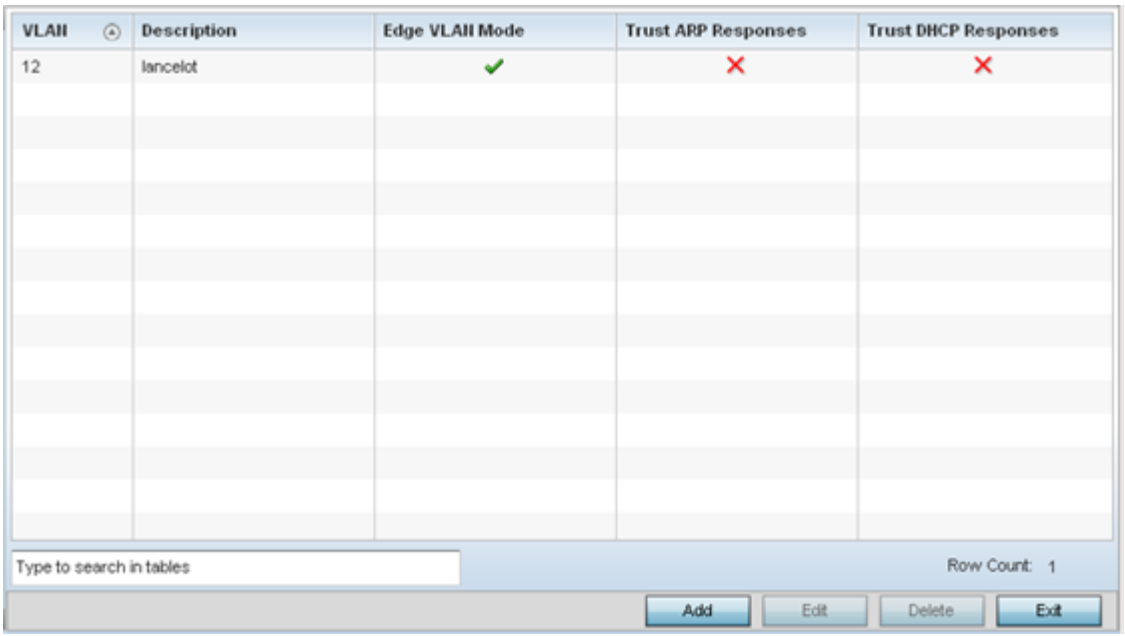
To define a bridge VLAN configuration:

1 Go to **Configuration → Devices → System Profile** .

The Profile screen displays. This screen lists access point profiles.

2 Select a profile from those listed on the screen. The selected profile's configuration menu displays.

3 Expand the **Network** node and select **Bridge VLAN**. The Bridge VLAN Main screen displays. This screen displays existing Bridge VLAN configurations.




4 Review the following VLAN configuration parameters to determine whether an update is warranted:

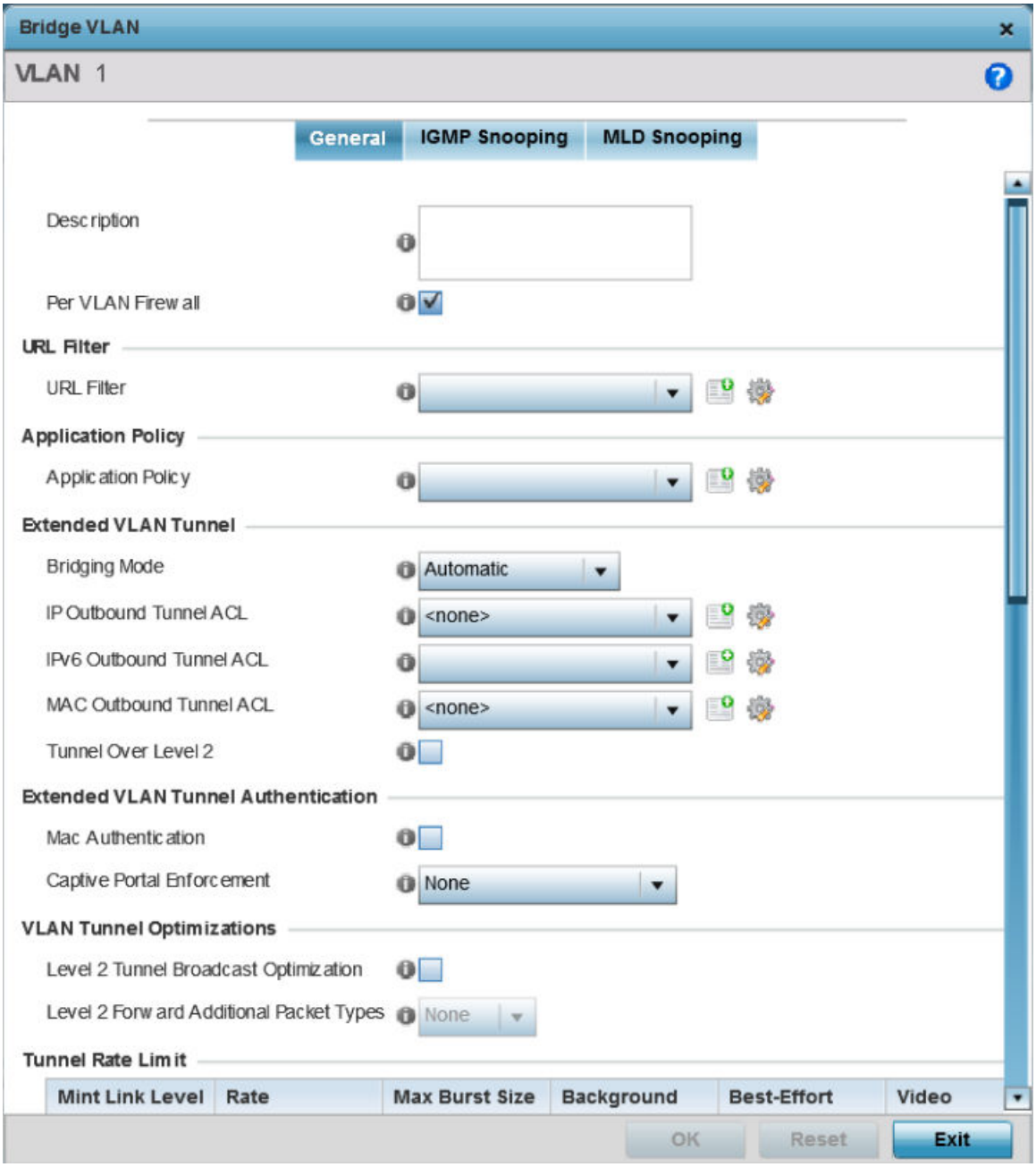
| | |
|---|---|
| VLAN | Lists the numerical identifier defined for the Bridge VLAN when initially created. The available range is from 1 - 4095. This value cannot be modified during the edit process. |
| Description | Lists a description of the VLAN assigned when it was created or modified. The description should be unique to the VLAN's specific configuration and help differentiate it from other VLANs with similar configurations. |
| Edge VLAN Mode | Defines whether the VLAN is currently in edge VLAN mode. A green checkmark defines the VLAN as extended. An edge VLAN is the VLAN where hosts are connected. For example, if VLAN 10 is defined with wireless clients, and VLAN 20 is where the default gateway resides, VLAN 10 should be marked as an edge VLAN and VLAN 20 shouldn't. When defining a VLAN as an edge VLAN, the firewall enforces additional checks on hosts in that VLAN. For example, a host cannot move from an edge VLAN to another VLAN and still keep firewall flows active. |
| Trust ARP Response | When ARP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks. |
| Trust DHCP Responses | When DHCP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. |

5 Select **Add** to define a new bridge VLAN configuration, **Edit** to modify an existing bridge VLAN configuration or **Delete** to remove a VLAN configuration.

### Bridge VLAN General Configuration

To define a bridge VLAN general configuration:

1 Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.




The General tab displays by default.

2 If adding a new Bridge VLAN configuration, use the spinner control to define a **VLAN** ID between 1 - 4094. This value must be defined and saved before the General tab can become enabled and the remainder of the settings defined. VLAN IDs 0 and 4095 are reserved and unavailable.

3 Set the following general bridge VLAN parameters:

| | |
|---|---|
| Description | If creating a new Bridge VLAN, provide a description (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations. |
| Per VLAN Firewall | Enable this setting to provide firewall allow and deny conditions over the bridge VLAN. This setting is enabled by default. |

4 Set or override the following URL Filter parameters. Web filters are used to control the access to resources on the Internet:

| | |
|---|---|
| URL Filter | Use the drop-down menu to select a URL filter to use with this Bridge VLAN. |

5 Set or override the following Application Policy parameters. Use the drop-down to select the appropriate Application Policy to use with this Bridge VLAN configuration.

6 Set the following Extended VLAN Tunnel parameters:

| | |
|---|---|
| Bridging Mode | Specify one of the following bridging modes for the VLAN.<br>*Automatic*: Select automatic to let the controller, service platform or access point determine the best bridging mode for the VLAN.<br>*Local*: Select Local to use local bridging mode for bridging traffic on the VLAN.<br>*Tunnel*: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN.<br>*isolated-tunnel*: Select isolated-tunnel to use a dedicated tunnel for bridging VLAN traffic. |
| IP Outbound Tunnel ACL | Select an IP Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound IP ACL is not available, select the *Create* button to make a new one. |
| MAC Outbound Tunnel ACL | Select a MAC Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound MAC ACL is not available click the Create button to make a new one. |
| Tunnel Over Level 2 | Select this option to allow VLAN traffic to be tunneled over level 2 links. This setting is disabled by default. |

**Note**

Local and Automatic bridging modes do not work with ACLs. ACLs can only be used with tunnel or isolated-tunnel modes.

7 Set the following Extended VLAN Tunnel Authentication settings:

| | |
|---|---|
| MAC Authentication | Select to enable source MAC authentication for extended VLAN and tunneled traffic (MiNT and L2TPv3) on this bridge VLAN. When enabled, it provides fast path authentications of clients, whose captive portal session has expired. This option is disabled by default. |
| Captive-Portal Authentication | Use the drop-down menu to specify authentication mode used for extended VLAN and tunneled traffic, on this Bridge VLAN. The options are:<br>**`None`** – No Authentication mode used. This is the default setting.<br>**`Authentication Failure`** – Configures MAC Authentication as the primary and Captive-Portal Authentication as the fall-back authentication mode.<br>**`Always`** – Configures Captive-Portal Authentication as the only mode of Authentication |
| Edge VLAN Mode | Select this option to enable edge VLAN mode. When selected, the edge controller's IP address in the VLAN is not used, and is now designated to isolate devices and prevent connectivity. This feature is enabled by default. |

8 Set the following Layer 2 Firewall parameters:

| | |
|---|---|
| Trust ARP Response | Select this option to use trusted ARP packets to update the DHCP Snoop Table to prevent IP spoof and arp-cache poisoning attacks. This feature is disabled by default. |
| Trust DHCP Responses | Select this option to use DHCP packets from a DHCP server as trusted and permissible within the managed network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. This feature is disabled by default. |
| Edge VLAN Mode | Select this option to enable edge VLAN mode. When selected, the edge controller's IP address in the VLAN is not used, and is now designated to isolate devices and prevent connectivity. This feature is enabled by default. |

9 Select the **OK** button to save the changes to the General tab. Select **Reset** to revert to the last saved configuration.

### Bridge VLAN IGMP Snooping

IGMP is used for managing IP multicast group members. Controllers and service platforms listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the controller or service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

To define a profile's bridge VLAN IGMP settings:

1 Select the **IGMP Snooping** tab.

2 Define the following General parameters for the bridge VLAN configuration:

| | |
|---|---|
| Enable IGMP Snooping | Select the check box to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the effective setting is disabled. |
| Forward Unknown Unicast Packets | Select the check box to enable to forward multicast packets from unregistered multicast groups. If disabled (the default setting), the unknown multicast forward feature is also disabled for individual VLANs. |
| Enable Fast Leave Processing | Select this option to remove a Layer 2 LAN interface from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network. |
| Last Member Query Count | Specify the number of group specific queries sent before removing an IGMP snooping entry. |

3 Within the Multicast Router section, select those interfaces used as multicast router interfaces. Multiple interfaces can be selected and overridden. Set the **`pim-dvmrp`** or **`static`** Multicast Routing Learn Mode. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths.

4 Set the following IGMP Querier parameters for the profile's bridge VLAN configuration:

| | |
|---|---|
| Enable IGMP Snooping | IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server, hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port. |
| Source IP Address | Define an IP address applied as the source address in the IGMP query packet. This address is used as the default VLAN querier IP address. |
| IGMP Version | Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. The default setting is 3. |
| Maximum Response Time | Specify the maximum time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. For IGMP reports from wired ports, reports are only forwarded to the multicast router ports. The default setting is 10 seconds. |
| Other Querier Timer Expiry | Specify an interval in either **Seconds** (60 - 300) or **Minutes** (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute. |

5 Select the **OK** button to save the changes to the bridge VLAN IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

### Bridge VLAN MLD Snooping

MLD *(Multicast Listener Discovery)* snooping enables a controller, service platform or access point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or access point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To set the MLD Snooping parameters:

1 Select the **MLD Snooping** tab.

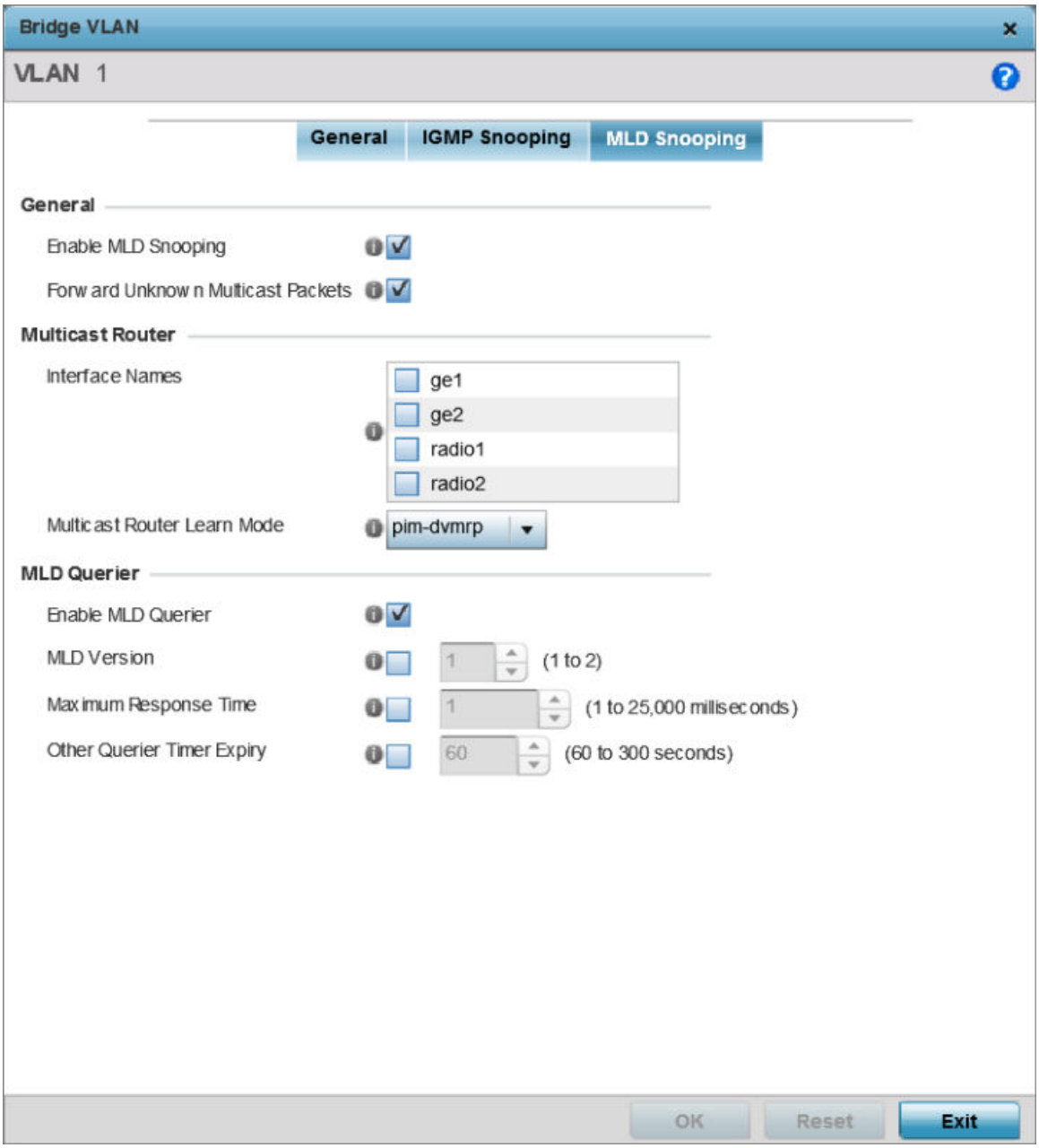



**Figure 69: Network Bridge VLAN screen, MLD Snooping tab**

2 Define the following General MLD snooping parameters for the Bridge VLAN configuration:

| | |
|---|---|
| Enable MLD Snooping | Enable MLD snooping to examine MLD packets and support content forwarding on this Bridge VLAN. Packets delivered are identified by a single multicast group address. Multicast packets are delivered using best-effort reliability, just like IPv6 unicast. MLD snooping is enabled by default. |
| Forward Unknown Packets | Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default. |

3 Define the following **Multicast Router** settings:

| | |
|---|---|
| Interface Names | Select the GE or radio interfaces used for MLD snooping. |
| Multicast Router Learn Mode | Set the pim-dvmrp or static multicast routing learn mode. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths. |

4 Set the following **MLD Querier** parameters for the profile's Bridge VLAN configuration:

| | |
|---|---|
| Enable MLD Querier | Select this option to enable MLD querier on the controller, service platform or access point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is enabled by default. |
| MLD Version | Define whether MLD version 1 or 2 is utilized with the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2. |
| Maximum Response Time | Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 1 milliseconds. |
| Other Querier Timer Expiry | Specify an interval in either Seconds (60 - 300) or Minutes (1 - 5) used as a timeout interval for other querier resources. The default setting is 60 seconds. |

5 Select the **OK** button located at the bottom right of the screen to save the changes.

Select **Reset** to revert to the last saved configuration.

### *Cisco Discovery Protocol Configuration*

CDP (Cisco Discovery Protocol) is a proprietary Data Link Layer protocol implemented in Cisco networking equipment. It's primarily used to obtain IP addresses of neighboring devices and discover their platform information. CDP is also used to obtain information about the interfaces the access point uses. CDP runs only over the data link layer enabling two systems that support different network-layer protocols to learn about each other.

To define the profile's CDP configuration:

1 Select the **Configuration → Devices → System Profile** tab from the Web UI.

The **Profile** screen displays. This screen lists the default and user-defined profiles.

2 Click **Add** to create a new profile. If modifying an existing profile, select the profile and click **Edit**.

To delete e profile, select it and click **Delete**.

The profile configuration menu displays.

3 Expand **Network** and select **Cisco Discovery Protocol**.

The CDP configuration screen displays.

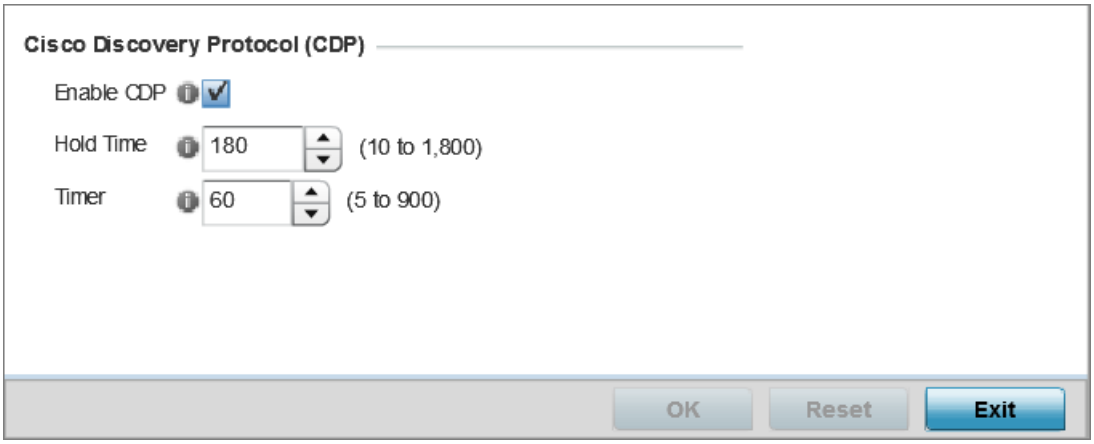



**Figure 70: Network - Cisco Discovery Protocol (CDP) screen**

4 Enable/disable CDP and set the following settings:

| | |
|---|---|
| Enable CDP | Select this option to enable CDP and allow for network address discovery of Cisco supported devices and operating system version. This setting is enabled by default. |
| Hold Time | Set a hold time (in seconds) for the transmission of CDP packets. Set a value from 10 - 1,800. The default setting is 1,800 seconds. |
| Timer | Use the spinner control to set the interval for CDP packet transmissions. The default setting is 60 seconds. |

5 Select **OK** to save the CDP configuration changes.

Select **Reset** to revert to the last saved configuration.

## *Link Layer Discovery Protocol Configuration*

The LLDP *(Link Layer Discovery Protocol)* provides a standard way for a controller or access point to advertise information about themselves to networked neighbors and store information they discover from their peers.

LLDP is neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about them to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management and connection endpoint information from adjacent devices.

Using LLDP, an access point is able to advertise its own identification, capabilities and media-specific configuration information and learn the same information from connected peer devices.

LLDP information is sent in an Ethernet frame at a fixed interval. Each frame contains one m LLDP PDU*(Link Layer Discovery Protocol Data Unit)*. A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

To set the LLDP configuration:

1 Select the **Configuration** → **Devices** → **System Profile** tab from the Web UI.

The Profile screen displays. This screen lists the default and user-defined profiles.

2 Click **Add** to create a new profile. If modifying an existing profile, select the profile and click **Edit**.

The profile configuration menu displays.

3 Expand the **Network** menu and select **Link Layer Discovery Protocol**.

To delete e profile, select it and click **Delete**.

The LLDP configuration menu displays.

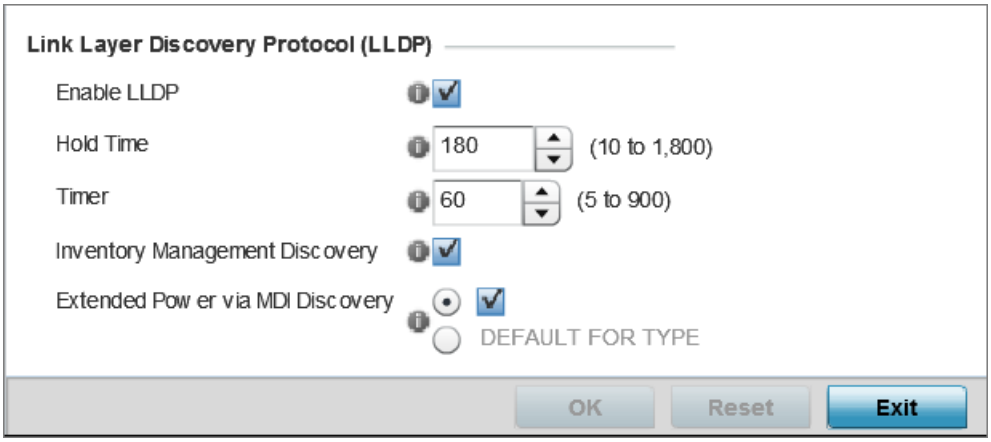



**Figure 71: Network - Link Layer Discovery Protocol (LLDP) screen**

4 Set the following LLDP parameters for the profile configuration:

| | |
|---|---|
| Enable LLDP | Select this option to enable LLDP on the access point. LLDP is enabled by default When enabled, an access point advertises its identity, capabilities and configuration information to connected peers and learns the same from them. |
| Hold Time | Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value from 10 - 1,800. The default hold time is 180 seconds. |
| Timer | Set the interval used to transmit LLDP PDUs. Define an interval from 5 - 900 seconds. The default setting is 60 seconds. |
| Inventory Management Discovery | Select this option to include LLPD-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default. |
| Extended Power via MDI Discovery | Select this option to include LLPD-MED extended power via MDI discovery TLV in LLDP PDUs. This setting is disabled by default. |

5 Select **OK** to save the LLDP configuration changes.

Select **Reset** to revert to the last saved configuration.

*Miscellaneous Network Configuration*

A profile can include a hostname within a DHCP lease for a requesting device. This helps an administrator track the leased DHCP IP address by hostname for the supported device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices.

To include hostnames in DHCP requests:

1 Select the **Configuration → Devices → System Profile** tab from the Web UI.
2 Expand the **Network** menu and select **Miscellaneous**.

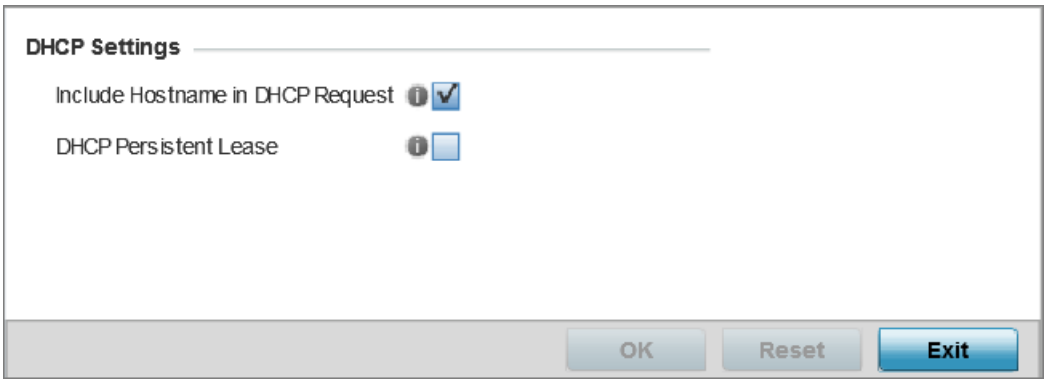



**Figure 72: Network - Miscellaneous screen**

3 Select the **Include Hostname in DHCP Request** option to include a hostname in a DHCP lease for a requesting device. This feature is enabled by default.
4 Select the **DHCP Persistent Lease** option to retain the lease that was last used by the access point if the access point's DHCP server resource were to become unavailable. This feature is enabled by default.
5 Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

*Aliases Overview*

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- Global aliases are defined from the **Configuration → Network → Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- Profiles aliases are defined from **Configuration → Devices → System Profile → Network → Alias**. These aliases are available for use to a specific group of wireless controllers or access points. Alias values defined in this profile override alias values defined within global aliases.

- RF Domain aliases are defined from **Configuration → Devices → RF Domain →Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- Device aliases are defined from **Configuration → Devices → Device Overrides → Network → Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an Network Alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the Network Alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the Network Alias works with the 172.16.10.0/24 network. Existing ACLs using this Network Alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Aliases can be classified as:

- Basic Alias
- Network Group Alias
- Network Service Alias

### Network Basic Alias

A *basic alias* is a set of configurations consisting of *VLAN*, *Host*, *Network*, *Address Range*, and *String* alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

To set a network basic alias configuration:

1 Go to **Configuration → Devices → System Profile** .

The Profile screen displays. This screen lists access point profiles.

2 Select a profile from the list.

The selected profile's configuration menu displays.

3 Expand the **Network** menu and select **Alias**.

The Basic Alias screen displays.

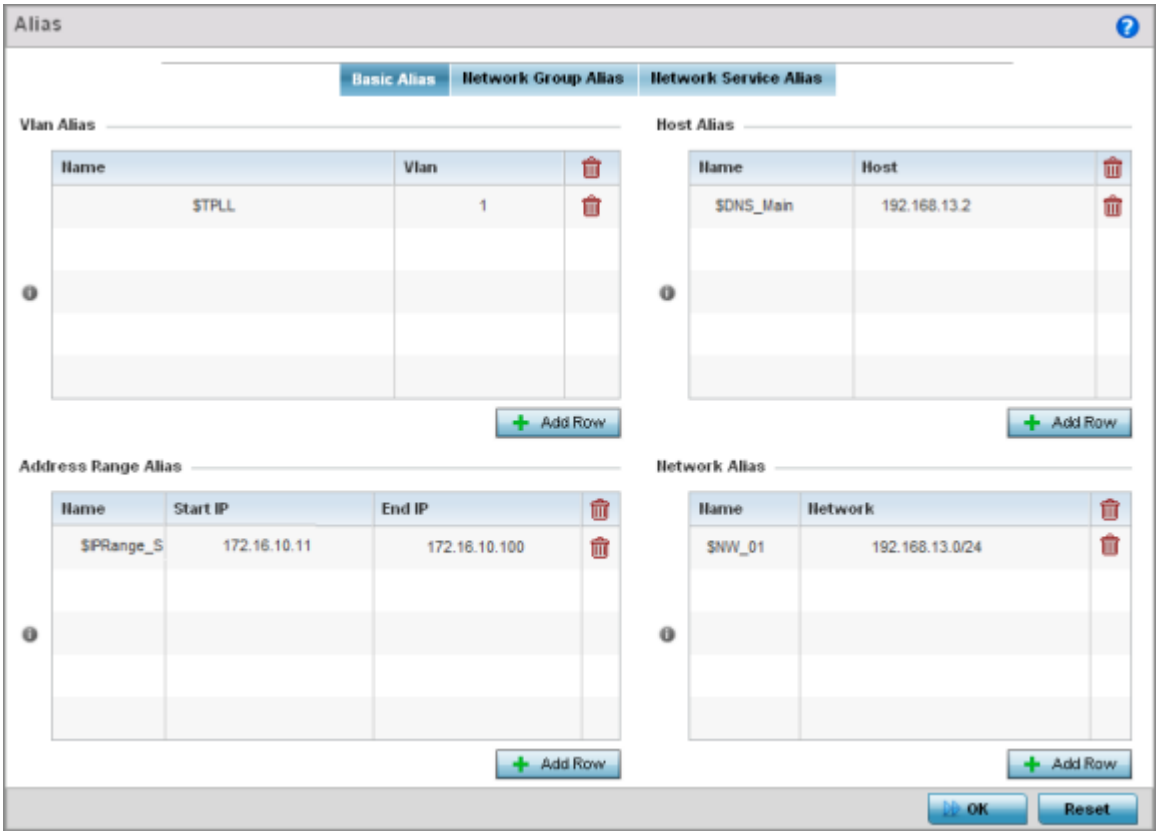



**Figure 73: Network - Basic Alias Screen**

4 Select **+ Add Row**, in the VLAN Alias table to add a VLAN alias settings.

VLANs aliases can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

| | |
|---|---|
| Name | If adding a new VLAN Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| VLAN | Use the spinner control to set a numeric VLAN from 1 - 4094. |

Note

A VLAN alias is used to replace VLANs in the following locations:

- Bridge VLAN
- IP Firewall Rules
- L2TPv3
- Switchport
- Wireless LANs

5 Select **+ Add Row**, in the **Address Range Alias** table to add an address range alias settings.

This option creates an alias for a range of IP address that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

| | |
|---|---|
| Name | If adding a new Address Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Start IP | Set a starting IP address used with a range of addresses utilized with the address range alias. |
| End IP | Set a ending IP address used with a range of addresses utilized with the address range alias. |

**Note**
An address range alias can be used to replace an IP address range in IP firewall rules.

6 Select **+ Add Row**, in the **Host Alias** table to add a host alias settings:

This option creates aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new Host Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Host | Set the IP address of the host machine. |

**Note**
A host alias can be used to replace hostnames in the following locations:

- IP Firewall Rules
- DHCP

7 Select **+ Add Row**, in the **Network Alias** table to add a network alias settings:

This option create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new Network Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Network | Provide a network address in the form of host/mask. |

Note

A network alias can be used to replace network declarations in the following locations:

- IP Firewall Rules
- DHCP

8 Select **+ Add Row**, in the String Alias table to add a string alias settings:

This option creates aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

| | |
|---|---|
| Name | If adding a new String Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Value | Provide a string value to use in the alias. |

Note

A string alias can be used to replace domain name stings in DHCP.

9 Click **OK** when completed to update the basic alias rules.

Click **Reset** to revert the screen back to its last saved configuration.

### Network Group Alias

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

A network group alias can be used in IP firewall rules to substitute hosts, subnets and IP address ranges.

To edit or delete a network alias configuration:

1 Select the **Network Group Alias** tab.

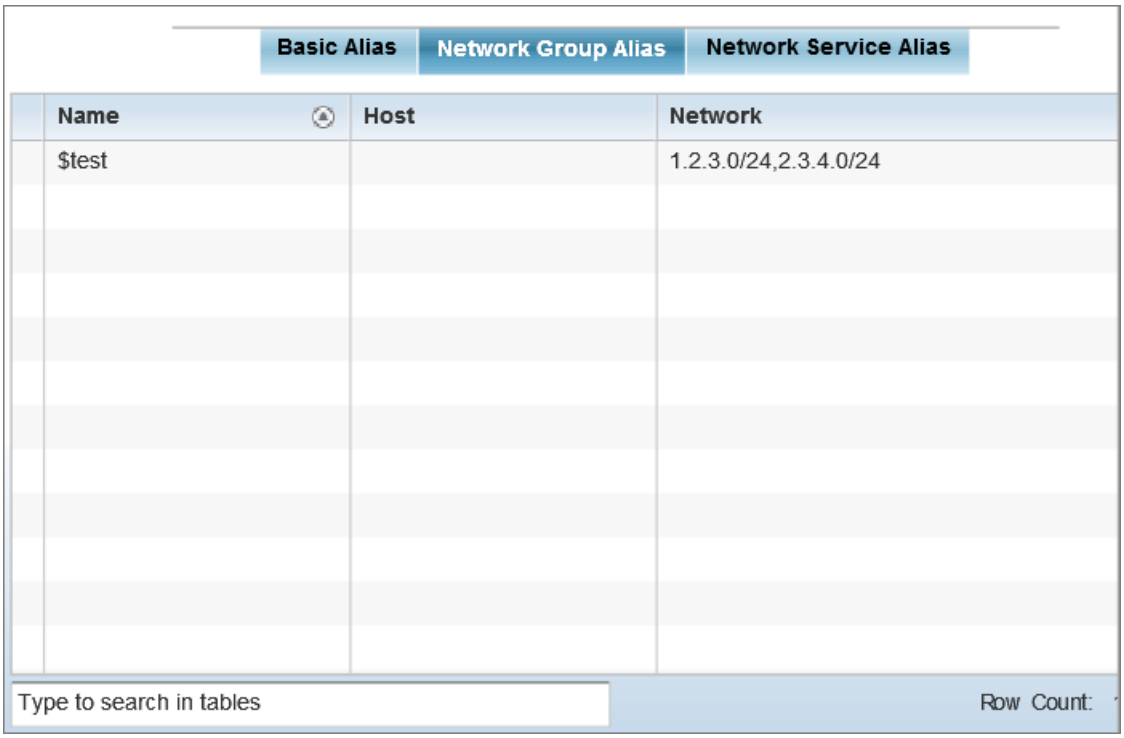



**Figure 74: Network Alias - Network Group Alias Screen**

2 Review the following to determine if a new alias configuration is needed or an existing configuration warrants modification:

| | |
|---|---|
| Name | Displays the administrator assigned name associated with the network group alias. |
| Host | Displays all the host aliases in the listed network group alias. Displays a blank column if no host alias is defined. |
| Network | Displays all network aliases in the listed network group alias. Displays a blank column if no network alias is defined. |

Adding and Editing Network Group Alias

You can add a new network group alias configuration or edit an existing configuration.

1 Select **Add** to create a new alias, **Edit** to modify the attributes of an existing alias, or **Delete** to remove obsolete aliases.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

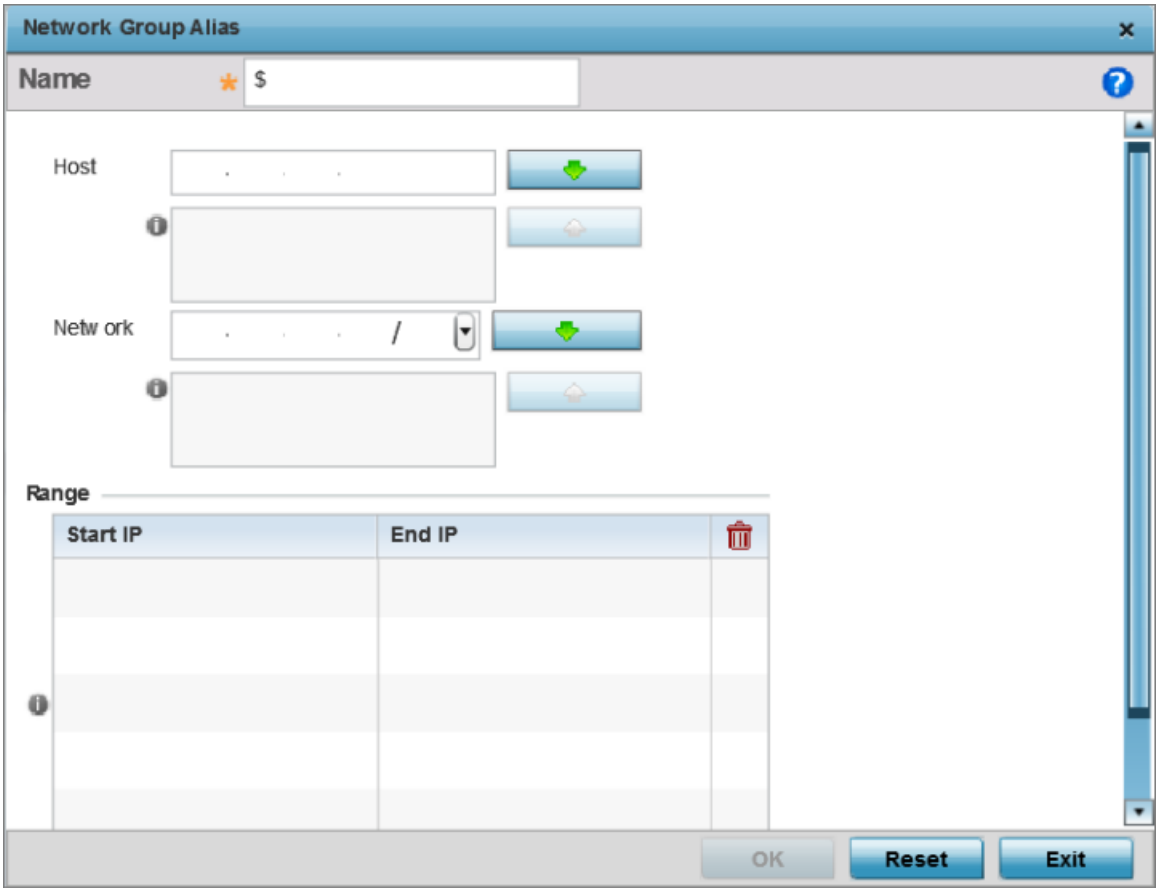



**Figure 75: Network Alias - Network Group Alias Add Screen**

2 If you are adding a new network alias rule, provide a `name` up to 32 characters. The network group alias name always starts with a dollar sign ($).

3 Define the following network group alias parameters:

| | |
|---|---|
| Host | Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table. |
| Network | Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table. |

4 Select **+ Add Row**, in the Range table to specify the Start IP address and End IP address for the alias range, or double-click on an existing alias range entry to edit it.

5 Select **OK** when completed to update the network group alias settings.

Select **Reset** to revert the screen to its last saved configuration.p

### Network Service Alias

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to two source port ranges and up to two destination port ranges can be configured. A maximum of four protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

A network service alias can be used to substitute protocols and ports in IP firewall rules.

To edit or delete a network service alias configuration:

Select the **Network Service Alias** tab.

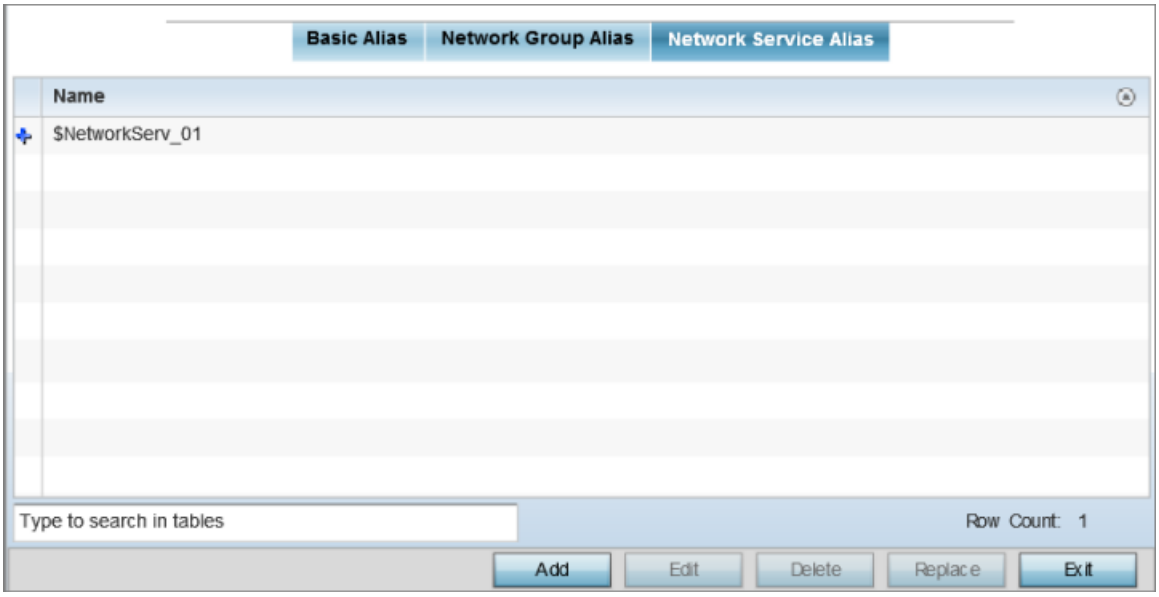



**Figure 76: Network Alias - Network Service Alias Screen**

Adding and Editing Network Service Alias

You can add a new network service alias configuration or edit an existing configuration.

1 Select **Add** to create a new network service alias.

Select an existing network service alias and click **Edit** to modify it. Select **Delete** to remove an existing network service alias from those available in the list.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

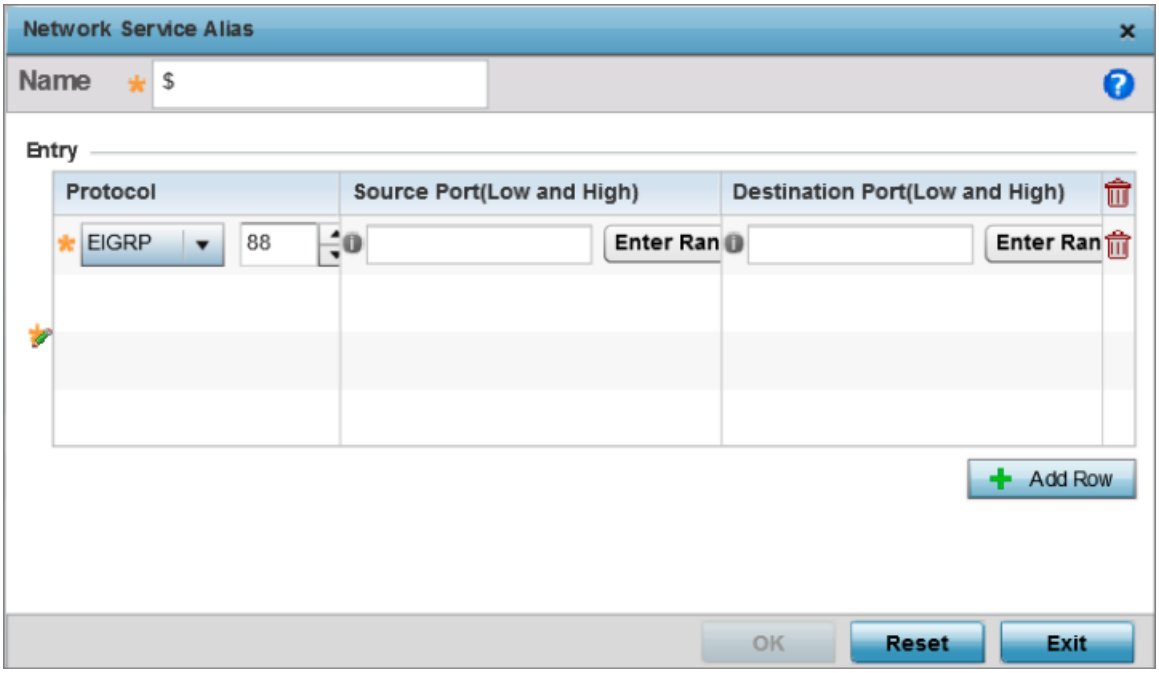



**Figure 77: Network Alias - Network Service Alias Add screen**

2 If you are adding a new Network Service Alias, give it a `Name` up to 32 characters to distinguish this alias configuration from others with similar attributes.

Note

The Network Service Alias name always starts with a dollar sign ($).

3 Select **+ Add Row**, in the Entry table and specify the following parameters:

| | |
|---|---|
| Protocol | Specify the protocol for which the alias is created. Use the drop down to select the protocol from **`eigrp`**, **`gre`**, **`icmp`**, **`igmp`**, **`ip`**, **`vrrp`**, **`igp`**, **`ospf`**, **`tcp`** and **`udp`**. Select **`other`** if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected. |
| Source Port (Low and High) | This field is relevant only if the protocol is *tcp* or *udp*.<br>Specify the source ports for this protocol entry. A range of ports can be specified. Select the **Enter Range** button next to the field to enter a lower and higher port range value. Up to eight (8) ranges can be specified. |
| Destination Port (Low and High) | This field is relevant only if the protocol is *tcp* or *udp*.<br>Specify the destination ports for this protocol entry. A range of ports can be specified. Select the **Enter Range** button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified. |

4 Select **OK** when completed to update the network service alias rules.

Select **Reset** to revert the screen back to its last saved configuration.

*IPv6 Neighbor Configuration*

IPv6 neighbor discovery uses ICMP messages and solicited multicast addresses to find the link layer address of a neighbor on the same local network, verify the neighbor's reachability and track neighboring devices.

Upon receiving a neighbor solicitation message, the destination replies with *neighbor advertisement* (NA). The source address in the NA is the IPv6 address of the device sending the NA message. The destination address in the neighbor advertisement message is the IPv6 address of the device sending the neighbor solicitation. The data portion of the NA includes the link layer address of the node sending the neighbor advertisement.

Neighbor solicitation messages also verify the availability of a neighbor once its the link layer address is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.

To set an IPv6 neighbor discovery configuration:

1 Go to **Configuration → Devices → System Profile** .

The Profile screen displays. This screen lists access point profiles.

2 Select a profile from the list.

The selected profile's configuration menu displays.

3 Expand **Network** menu and select **IPv6 Neighbor**.

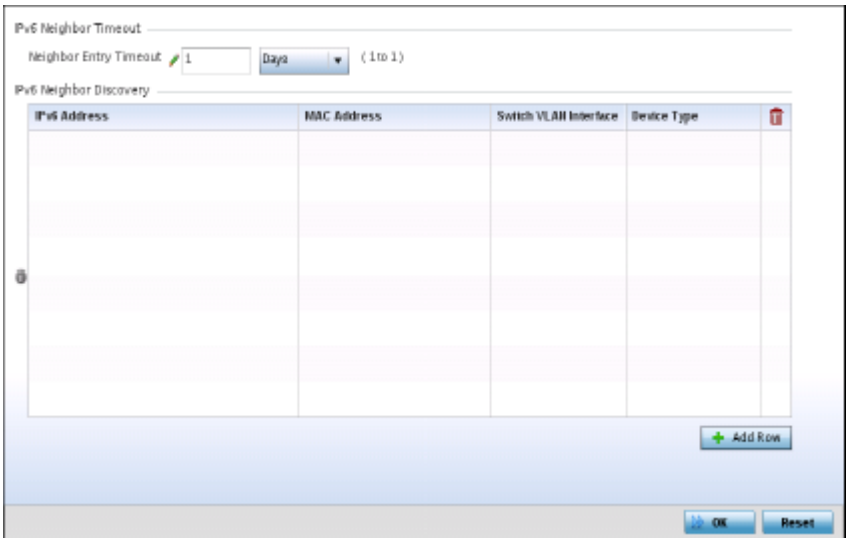



**Figure 78: IPv6 Neighbor screen**

4 Set an **IPv6 Neighbor Entry Timeout** in either **`Seconds`** (15 - 86,400), **`Minutes`** (1 - 1,440), **`Hours`** (1 - 24) or **`Days`** (1). The default setting is 1 hour.

5 Select **+ Add Row**, in the IPv6 Neighbor Discovery table to define the following:

| | |
|---|---|
| IPv6 Address | Provide a static IPv6 IP address for neighbor discovery. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the Neighbor Discovery Protocol via ICMPv6 *(Internet Control Message Protocol version 6)* router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| MAC Address | Enter the hardware encoded MAC addresses of up to 256 IPv6 neighbor devices. A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable. |
| Switch VLAN Interface | Use the spinner control to set the virtual interface (from 1 - 4094) used for neighbor advertisements and solicitation messages. |
| Device Type | Specify the device type for this neighbor solicitation is for. Options include Host, Router and DHCP Server. The default setting is Host. |

**Note**

A maximum of 256 neighbor entries can be defined.

6 Select **OK** to save the changes.

Select **Reset** to revert to the last saved configuration.

## Profile Security Configuration

An access point profile can have its own firewall policy, wireless client role policy, WEP shared key authentication and NAT policy applied.

Before defining a profile's security configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Ensure the contents of the certificate revocation list are periodically audited to ensure revoked certificates remained quarantined or validated certificates are reinstated.
- NAT alone does not provide a firewall. If deploying NAT on a profile, add a firewall on the profile to block undesirable traffic from being routed. For outbound Internet access, a stateful firewall can be configured to deny all traffic. If port address translation is required, a stateful firewall should be configured to only permit the TCP or UDP ports being translated.

For more information, refer to the following:


- Defining Profile VPN Settings on page 217
- Defining Profile Auto IPSec Tunnel Settings on page 234
- Defining Profile Security Settings on page 235
- Setting the Certificate Revocation List (CRL) Configuration on page 237
- Setting the RADIUS Trustpoint Configuration on page 238
- Setting the NAT Configuration on page 238

- Bridge NAT Configuration on page 247
- Defining Profile Application Visibility Settings on page 250


### *Defining Profile VPN Settings*

IPSec VPN provides a secure tunnel between two networked peer controllers or service platforms. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of SA *(security associations)* between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Use *crypto maps* to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include transform sets. A *transform set* is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

IKE *(Internet Key Exchange)* protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual preconfiguration.

To define a profile's VPN settings:

1 Select **Configuration → Devices → System Profile**.

A list of profiles displays in the right-hand UI.

2 Select a profile from the list.

The profile configuration menu displays.

3 Expand the **Security** menu and select **VPN**.

The VPN configuration's IKE Policy screen displays by default.

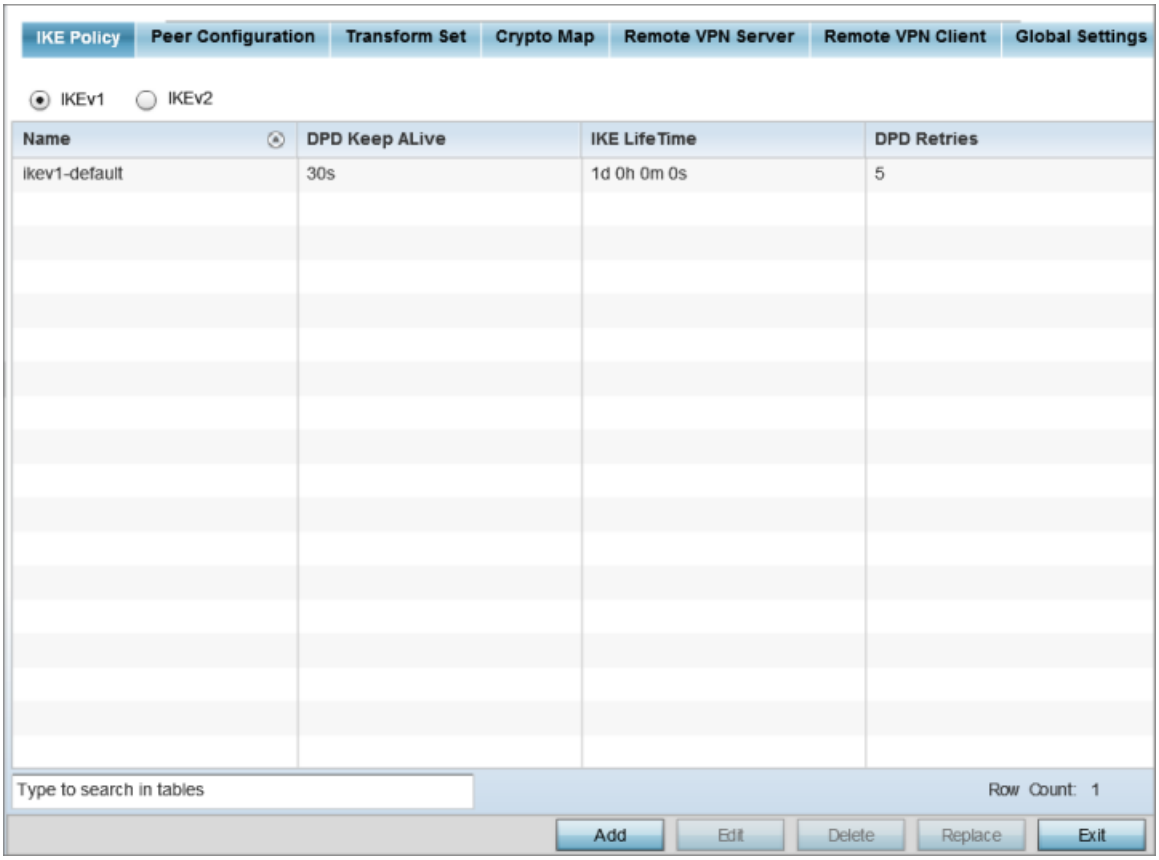



**Figure 79: Profile Security - VPN IKE Policy Screen**

4 Select either **IKEv1** or **IKEv2** to enforce VPN peer key exchanges using either IKEv1 or IKEv2.

IKEv2 is recommended in most deployments. IKEv2 provides improvements from the original IKEv1 design – for example, improved cryptographic mechanisms, NAT and firewall traversal, and attack resistance.

The appearance of the IKE Policy screens differs depending on whether IKEv1 or IKEv2 mode is selected.

5 Refer to the following to determine whether an IKE Policy requires creation, modification, or removal:

| | |
|---|---|
| Name | The 32-character maximum name assigned to the IKE policy. |
| DPD Keep Alive | Lists each policy's IKE keep alive message interval defined for IKE VPN tunnel dead peer detection. |

| | |
|---|---|
| IKE LifeTime | Displays each policy's lifetime for an IKE SA. The lifetime defines how long a connection (encryption/authentication keys) should last, from successful key negotiation to expiration. Two peers need not exactly agree on the lifetime, though if they do not, there is some clutter for a superseded connection on the peer defining the lifetime as longer. |
| DPD Retries | Lists each policy's number maximum number of keep alive messages sent before a VPN tunnel connection is defined as dead by the peer.<br><br>Note:<br>This option only appears when IKEv1 is selected. |

### Adding Editing IKEv1 Policy

You can add a new IKEv1 Policy of edit and existing policy.

1 Click **Add** to define a new IKEv1 Policy configuration, **Edit** to modify an existing configuration, or **Delete** to remove an existing configuration.

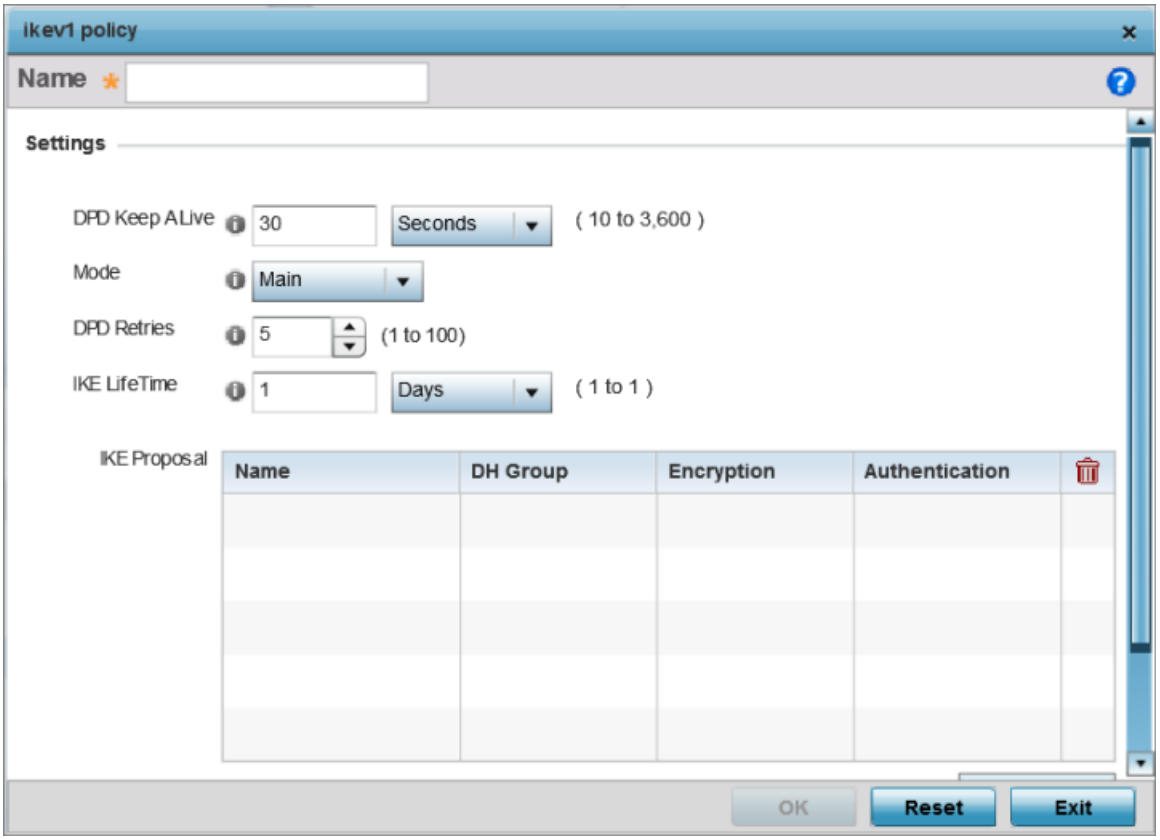



**Figure 80: Profile Security - IKE Policy - Add/Edit Screen**

2 If you are creating a new IKEv1 policy, assign it a 32-character maximum **Name** to help differentiate this IKE configuration from others with similar parameters.

3 Configure the following IKEv1 settings:

| | |
|---|---|
| DPD Keep Alive | Configure the IKE keep alive message interval used for dead peer detection on the remote end of the IPSec VPN tunnel. Set this value in either **seconds (10 - 3,600)**, **minutes (1 - 60)**, or **hours (1)**. The default setting is 30 seconds. This setting is required for both IKEv1 and IKEV2. |
| Mode | If you are using IKEv1, define the IKE mode as either **Main** or **Aggressive**. IPSEC has two modes in IKEv1 for key exchanges. Aggressive mode requires 3 messages be exchanged between the IPSEC peers to set up the SA, Main requires 6 messages. The default setting is Main. |
| DPD Retries | Set the maximum number of keep alive messages sent before a VPN tunnel connection is defined as dead. The available range is from 1 - 100. The default setting is 5. |
| IKE LifeTime | Set the lifetime defining how long a connection (encryption/authentication keys) should last from successful key negotiation to expiration. Set this value in either seconds (600 - 86,400), minutes (10 - 1,440), hours (1 - 24), or days (1). This setting is required for both IKEv1 and IKEv2. |

4 Click **+Add Row**, in the IKE Proposal table to define the network address of a target peer and its security settings.

| | |
|---|---|
| Name | If you are creating a new IKE policy, assign the target peer (tunnel destination) a 32-character maximum name to distinguish it from others with a similar configuration. |
| DH Group | Define a DH *(Diffie-Hellman)* identifier used by the VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include 2, 5 and 14. The default setting is 5. |
| Encryption | Select an encryption method used by the tunnelled peers to securely interoperate. Options include **3DES**, **AES**, **AES-192**, and **AES-256**. The default setting is AES-256. |
| Authentication | Select an authentication hash algorithm used by the peers to exchange credential information. Options include **SHA**, **SHA256**, and **MD5**. The default setting is SHA. |

5 Click **OK** to save the changes made in the IKE Policy screen.

Click **Reset** to revert to the last saved configuration. Click the **Delete Row** icon as needed to remove a peer configuration.

6 Click **+Add Row** in the IKE Proposal table to define the network address of a target peer and its security settings.

| | |
|---|---|
| Name | If you are creating a new IKE policy, assign the target peer (tunnel destination) a 32-character maximum name to distinguish it from others with a similar configuration. |
| DH group | Define a DH identifier used by the VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include 2, 5 and 14. The default setting is 5. |
| Encryption | Select an encryption method used by the tunnelled peers to securely interoperate. Options include **3DES**, **AES**, **AES-192** and **AES-256**. The default setting is AES-256. |
| Authentication | Select an authentication hash algorithm used by the peers to exchange credential information. Options include **SHA**, **SHA256** and **MD5**. The default setting is SHA. |

7 Click **OK** to save the changes made in the IKE Policy screen.

Click **Reset** to revert to the last saved configuration. Click the **Delete Row** icon as needed to remove a peer configuration.p

### Adding Editing IKEv2 Policy

You can add a new IKEv2 Policy of edit and existing policy.

1 Select **Add** to define a new IKEv2 Policy configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing configuration.

2 If you are creating a new IKEv2 policy, assign it a 32-character maximum **Name** to help differentiate this IKE configuration from others with similar parameters.

3 Configure the following IKEv2 settings:

| | |
|---|---|
| Name | If creating a new IKE policy, assign it a 32 character maximum name to help differentiate this IKE configuration from others with similar parameters. |
| DPD Keep Alive | Configure the IKE keep alive message interval used for dead peer detection on the remote end of the IPSec VPN tunnel. Set this value in either *Seconds* (10 - 3,600), *Minutes* (1 - 60) or *Hours* (1). The default setting is 30 seconds. This setting is required for both IKEv1 and IKEV2. |
| IKE LifeTime | Set the lifetime defining how long a connection (encryption/authentication keys) should last from successful key negotiation to expiration. Set this value in either *Seconds* (600 - 86,400), *Minutes* (10 - 1,440), *Hours* (1 - 24) or *Days* (1). This setting is required for both IKEv1 and IKEV2. |

4 Click **+Add Row**, in the IKE Proposal table to define the network address of a target peer and its security settings.

| | |
|---|---|
| Name | If creating a new IKE policy, assign the target peer (tunnel destination) a 32 character maximum name to distinguish it from others with a similar configuration. |
| DH Group | Use the drop-down menu to define a DH *(Diffie-Hellman)* identifier used by the VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include 2, 5 and 14. The default setting is 5. |
| Encryption | Select an encryption method used by the tunneled peers to securely interoperate. Options include *3DES*, *AES*, *AES-192* and *AES-256*. The default setting is AES-256. |
| Authentication | Select an authentication hash algorithm used by the peers to exchange credential information. Options include *SHA* and *MD5*. The default setting is SHA. |

5 Select **OK** to save the changes made within the IKE Policy screen.

Select **Reset** to revert to the last saved configuration. Select the **Delete Row** icon as needed to remove a peer configuration.

### Peer Configuration

To add a new peer configuration or edit an existing peer configuration.

1 Select the **Peer Configuration** tab to assign additional network address and IKE settings to the intended VPN tunnel peer destination.

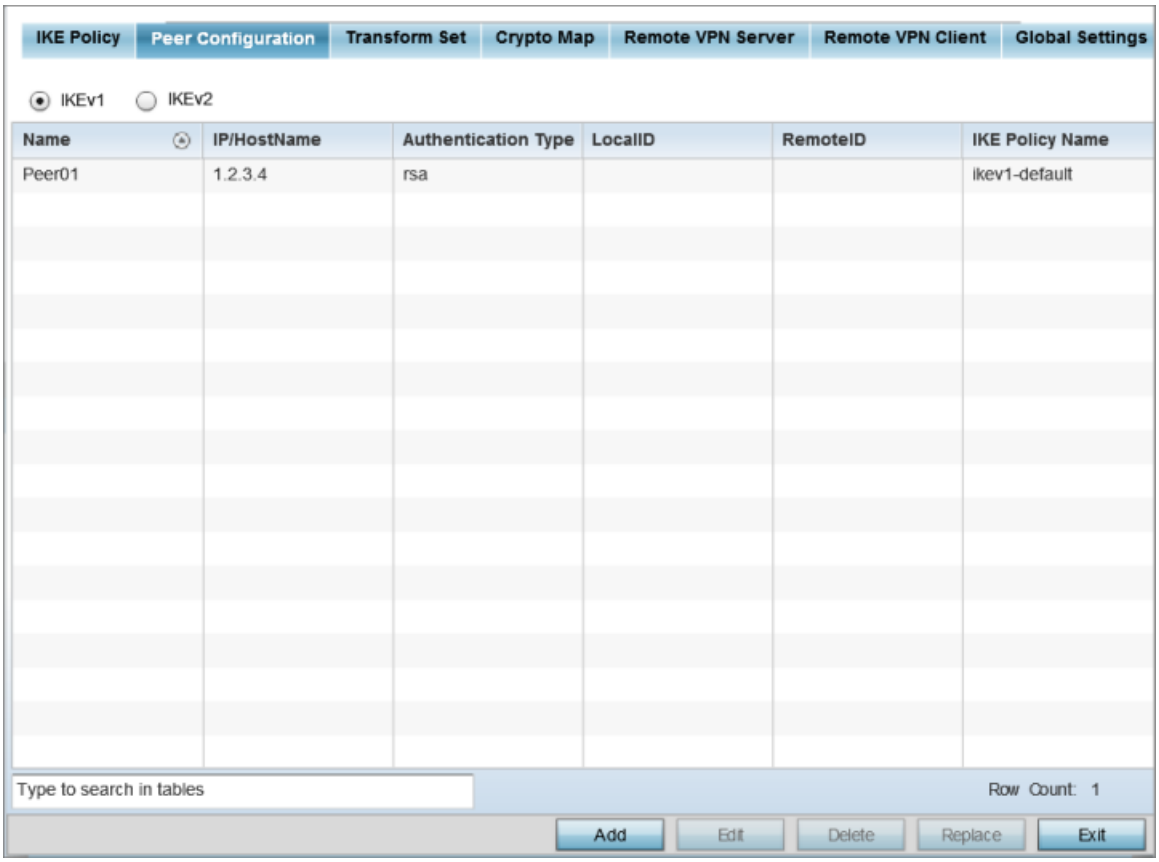



**Figure 81: Profile Security - VPN Peer Destination Screen (IKEv1 Example)**

2 Select either **IKEv1** or **IKEv2** to enforce VPN key exchanges using either IKEv1 or IKEv2.

3 Refer to the following to determine whether a new VPN peer configuration requires creation, an existing configuration requires modification, or a configuration requires removal.

| | |
|---|---|
| Name | Lists the 32-character maximum name assigned to each listed peer configuration at the time of its creation. |
| Hostname/IP | The IP address (or host address FQDN) of the IPSec VPN peer targeted for secure tunnel connection and data transfer. |
| Authentication Type | Whether the peer configuration has been defined to use PSK *(pre-shared key)* or RSA *(Rivest, Shamir, and Adleman)*. RSA is an algorithm for public key cryptography. It is the first algorithm known to be suitable for both signing and encryption. If you are using IKEv2, this screen displays both local and remote authentication, because both ends of the VPN connection require authentication. |
| Local id | The local identifier used within this peer configuration for an IKE exchange with the target VPN IPSec peer. |
| Remote id | The means by which the target remote peer is to be identified (for example, string or FQDN) within the VPN tunnel. |
| IKE Policy Name | The IKEv1 or IKE v2 policy used with each listed peer configuration. |

Insert ing title

To add or edit an IKev1 or IKEv2 peer configuration.

1 Select either **IKEv1** or **IKEv2** to enforce VPN key exchanges using either IKEv1 or IKEv2.

2 Click **Add** to define a new peer configuration, **Edit** to modify an existing configuration, or **Delete** to remove an existing peer configuration.

The parameters that can de defined for the peer configuration vary depending on whether IKEv1 or IKEv2 was selected.

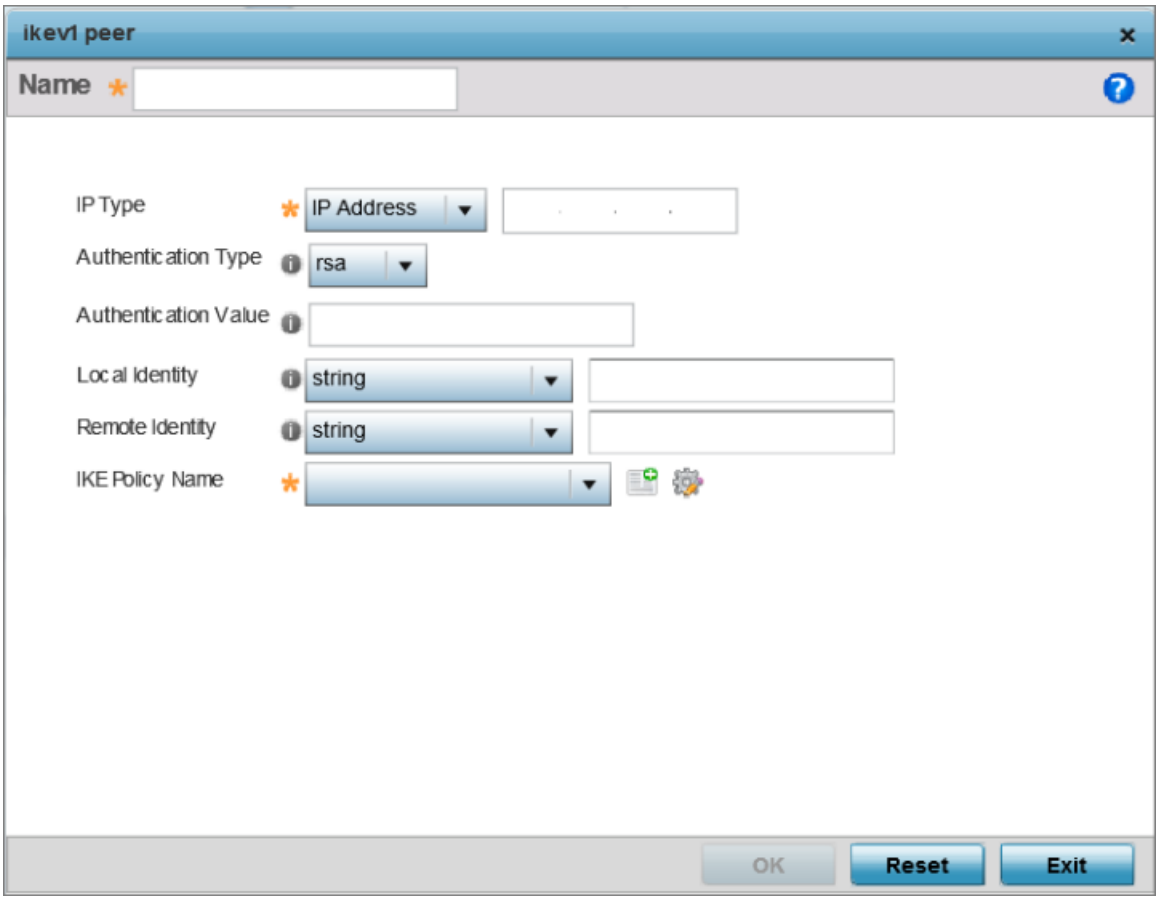



**Figure 82: Profile Security - VPN IKE Policy - Add IKE Peer Screen**

| | |
|---|---|
| Name | If you are creating a new peer configuration (remote gateway) for VPN tunnel connection, assign it a 32-character maximum name to distinguish it from other with similar attributes. |
| IP Type | Enter either the **`IP address`** or the **`FQDN`** hostname of the IPSec VPN peer used in the tunnel setup. A hostname cannot exceed 64 characters. |
| Authentication Type | Select the authentication type used by the VPN peer. The options are: **`PSK`** or **`rsa`**. RSA is an algorithm for public key cryptography. It is the first algorithm known to be suitable for signing and encryption If using IKEv2, this screen displays both local and remote authentication options, because both ends of the VPN connection require authentication.<br>RSA is the default value for both local and remote authentication, regardless of whether IKEv1 or IKEv2 is used. |

| | |
|---|---|
| Authentication Value | Define the authentication string (shared secret) shared by both ends of the VPN tunnel connection. The string must be between 8 - 21 characters long. If using IKEv2, both a local and remote string must be specified for handshake validation at both ends (local and remote) of the VPN connection. |
| Local Identity | Select the local identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include **IP Address**, **Distinguished Name**, **FQDN**, **email**, **string**, **autogen-uniqueid**. The default setting is string. |
| Remote Identity | Select the remote identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include **IP Address**, **Distinguished Name**, **FQDN**, **email**, and **string**. The default setting is string. |
| IKE Policy Name | Select the IKEv1 or IKE v2 policy name (and settings) to apply to this peer configuration. If you need to create a new policy, click the **Create** icon. |

3 Click **OK** to save the changes made in the peer configuration screen.

Click **Reset** to revert to the last saved configuration.

### Transform Set Configuration

A *transform set* is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

1 Select the **Transform Set** tab.

Create or modify transform set configurations to specify how traffic is protected.

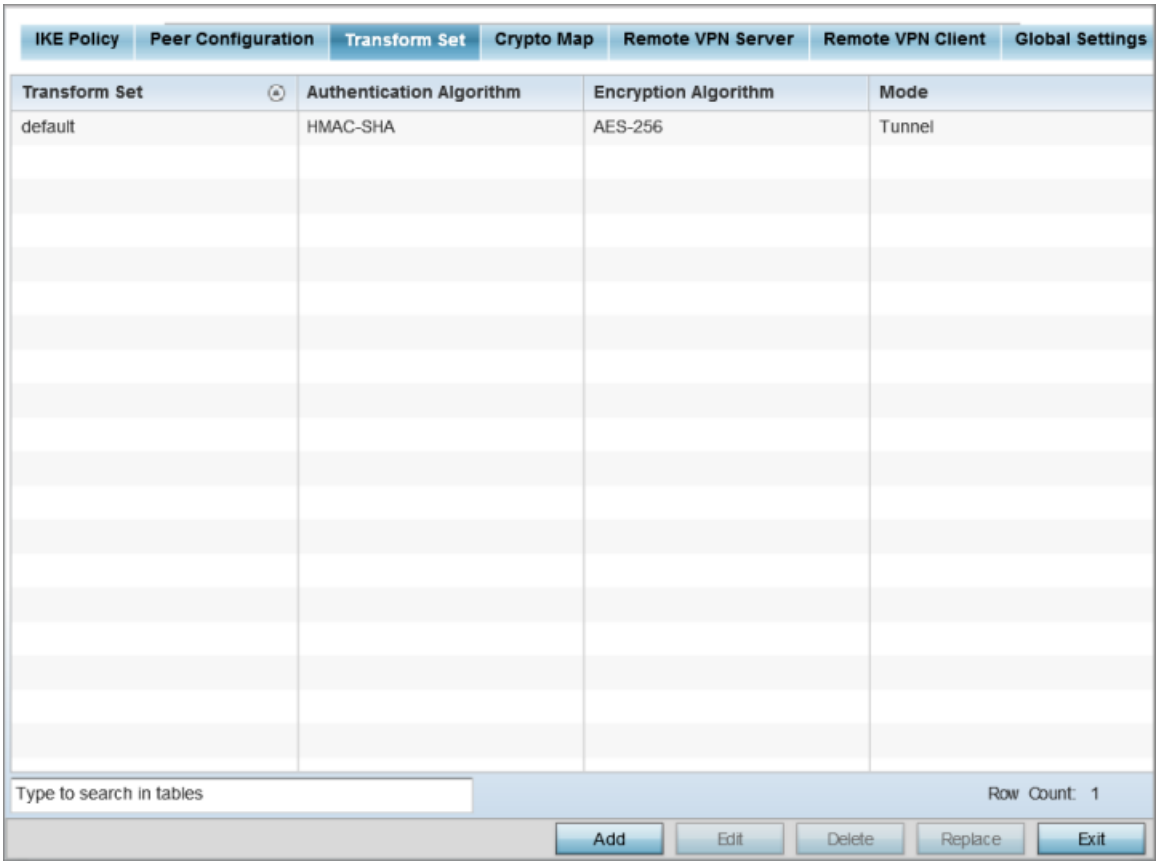



**Figure 83: Profile Security - VPN Transform Set Screen**

2 Review the following attributes of existing Transform Set configurations:

| | |
|---|---|
| Name | The 32-character maximum name assigned to each listed transform set upon creation. A transform set is a combination of security protocols, algorithms, and other settings applied to IPSec protected traffic. |
| Authentication Algorithm | Lists each transform sets's authentication scheme used to validate identity credentials. The authentication scheme is either **HMAC-SHA** or **HMAC-MD5**. |
| Encryption Algorithm | Displays each transform set's encryption method for protecting transmitted traffic. |
| Mode | Displays either **Tunnel** or **Transport** as the IPSec tunnel type used with the transform set. **Tunnel** is used for site-to-site VPN and **Transport** should be used for remote VPN deployments. |

3

4

Additing Editing Transform Set

You can add a new transform set or edit an existing transform set configuration.

1 Click **Add** to define a new transform set configuration, **Edit** to modify an existing configuration, or **Delete** to remove an existing transform set.

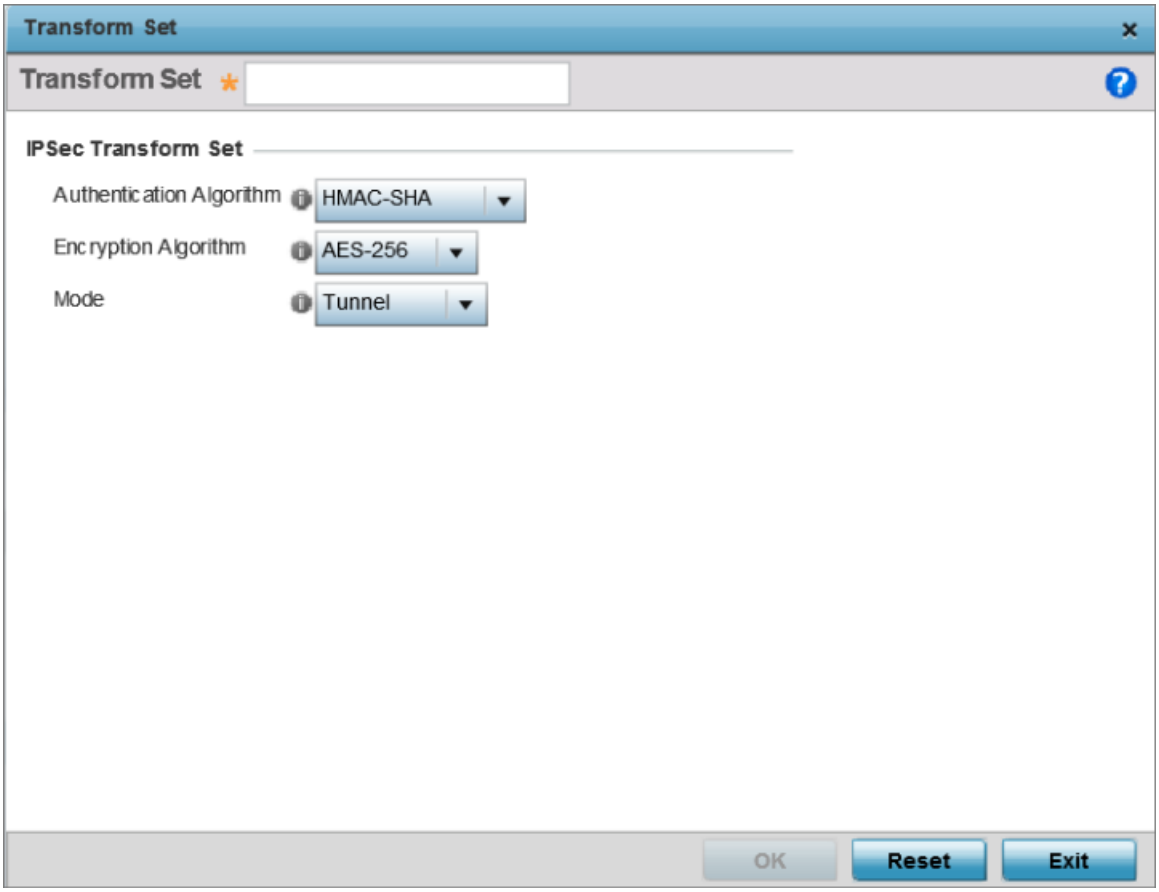



**Figure 84: Profile Security - VPN Transform Set Create/Modify Screen**

2 Define the following settings for the new or modified transform set configuration:

| | |
|---|---|
| Name | If you are creating a new transform set, define a 32-character maximum name to differentiate this configuration from others with similar attributes. |
| Authentication Algorithm | Set the transform sets's authentication scheme used to validate identity credentials. Use the drop-down menu to select either **HMAC-SHA**, **HMAC-MD5**, **sha256-hmac** or **aes-xcbc-mac**. The default setting is HMAC-SHA. |
| Encryption Algorithm | Set the transform set encryption method for protecting transmitted traffic. Options include **DES**, **3DES**, **AES**, **AES-192**, and **AES-256**. The default setting is AES-256. |
| Mode | Select either **Tunnel** or **Transport** as the IPSec tunnel type used with the transform set. The Tunnel option is used for site-to-site VPN and Transport is used for remote VPN deployments. The default setting is Tunnel. |

3 Click **OK** to save the changes made in the Transform Set screen.
Click **Reset** to revert to the last saved configuration.

### Crypto Map Configuration

Use *crypto maps* to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include transform sets. A *transform set* is a combination of security protocols,

algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

1 Select the **Crypto Map** tab. Use crypto maps (as applied to IPSec VPN) to combine the elements used to create IPSec SAs (including transform sets).

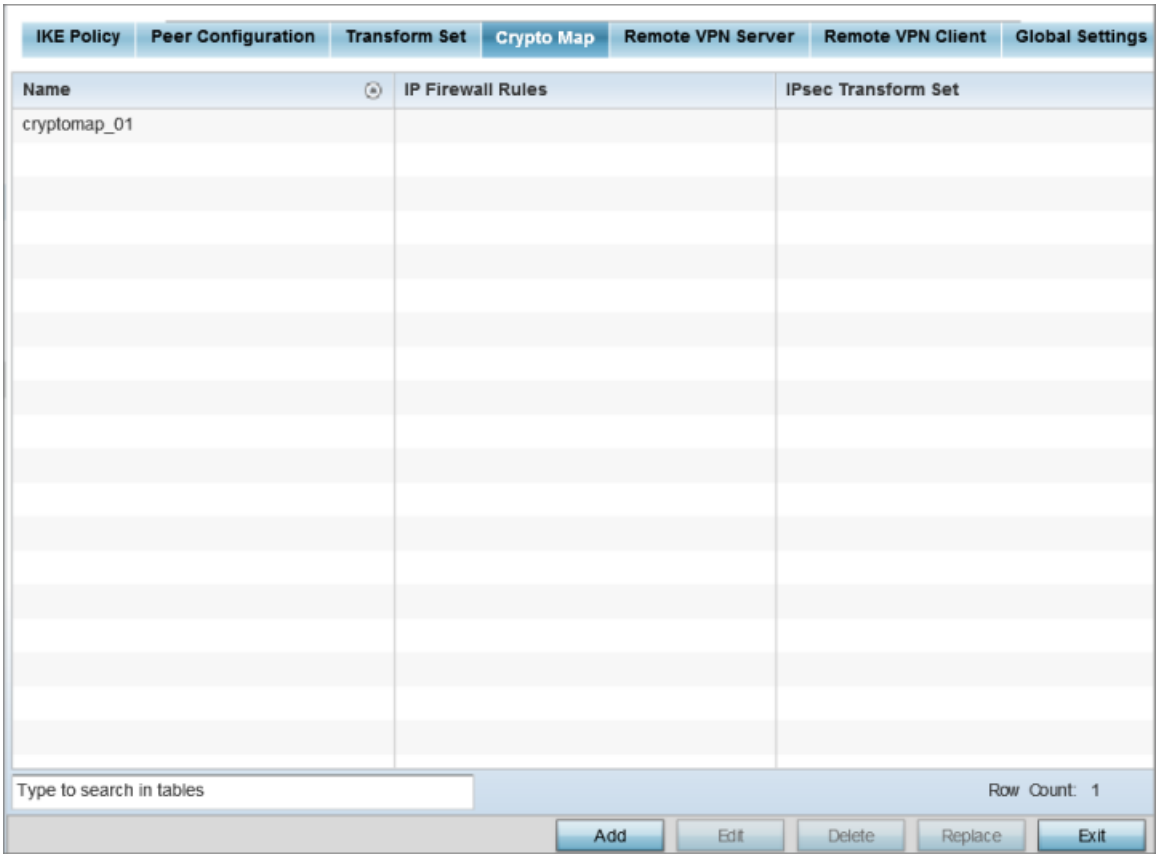



**Figure 85: Profile Security - Crypto Map tab**

2 Review the following configuration parameters to assess existing crypto map relevance:

| | |
|---|---|
| Name | Lists the 32 character maximum name assigned for each crypto map upon creation. This name cannot be modified as part of the edit process. |
| IP Firewall Rules | Lists the IP firewall rules defined for each displayed crypto map configuration. Each firewall policy contains a unique set of access/deny permissions applied to the VPN tunnel and its peer connection. |
| IPSec Transform Set | Displays the transform set (encryption and has algorithms) applied to each listed crypto map configuration. Thus, each crypto map can be customized with its own data protection and peer authentication schemes. |

Addinting Editing Crypto Map

You can add a new crypto map or edit an existing crypto map.

1 If requiring a new crypto map configuration, select the **Add** button. If updating the configuration of an existing crypto map, select it from amongst those available and select the **Edit** button.

2 If adding a new crypto map, assign it a `name` up to 32 characters as a unique identifier. Select the **Continue** button to proceed to the VPN Crypto Map screen.

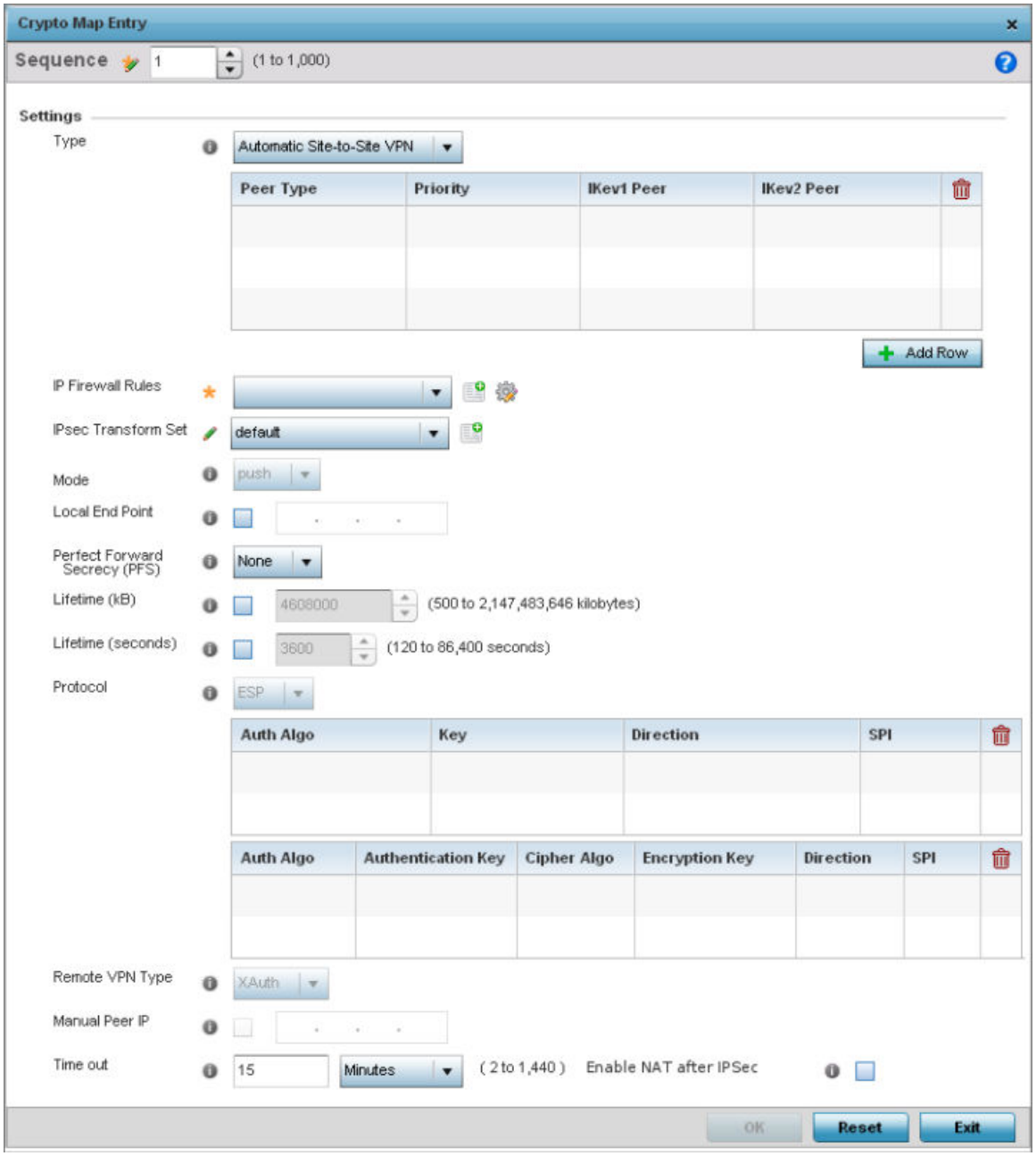



**Figure 86: Profile Security - VPN Crypto Map Entry Screen**

3 Define the following parameters to set the crypto map configuration:

| | |
|---|---|
| Sequence | Each crypto map configuration uses a list of entries based on a sequence number. Specifying multiple sequence numbers within the same crypto map extends connection flexibility to multiple peers on the same interface, based on this selected sequence number (from 1 - 1,000). |
| Type | Define the site-to-site-manual, site-to-site-auto or remote VPN configuration defined for each listed crypto map configuration. |

| | |
|---|---|
| IP Firewall Rules | Use the drop-down menu to select the ACL used to protect IPSec VPN traffic. New access/deny rules can be defined for the crypto map by selecting the **Create** icon, or an existing set of firewall rules can be modified by selecting the **Edit** icon. |
| IPSec Transform Set | Select the transform set (encryption and hash algorithms) to apply to this crypto map configuration. |
| Mode | Use the drop-down menu to define which mode (pull or push) is used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push. |
| Local End Point | Select this option to define an IP address as a local tunnel end-point address. This setting represents an alternative to an interface IP address. |
| Perfect Forward Secrecy (PFS) | PFS is key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must not be used to derive any additional keys. Options include None, 2, 5 and 14. The default setting is None. |
| Lifetime (KB) | Select this option to define a connection volume lifetime (in kilobytes) for the duration of an IPSec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes. |
| Lifetime (seconds) | Select this option to define a lifetime (in seconds) for the duration of an IPSec VPN security association. Once the set value is exceeded, the association is timed out. The available range is from 120 - 86,400 seconds. The default setting is 120 seconds. |
| Protocol | Select the security protocol used with the VPN IPSec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include ESP and AH. The default setting is ESP. |
| Remote VPN Type | Define the remote VPN type as either None or XAuth. XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device respond with a failed or passed message. The default setting is XAuth. |
| Manual Peer IP | Select this option to define the IP address of an additional encryption/ decryption peer. |
| Time Out | Select this option to set the IPSec SA time out value. Use the textbox and the drop-down list to configure the time out duration. |
| Enable NAT after IPSec | Select this option to enable NAT after IPSec. Enable this if there are NATted networks behind VPN tunnels. |

4 Select **OK** to save the updates made to the Crypto Map Entry screen.

Selecting **Reset** reverts the screen to its last saved setting.

### Remote VPN Server Configuration

To configure the remote VPN server settings:

1 Select Remote VPN Server.

Use this screen to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

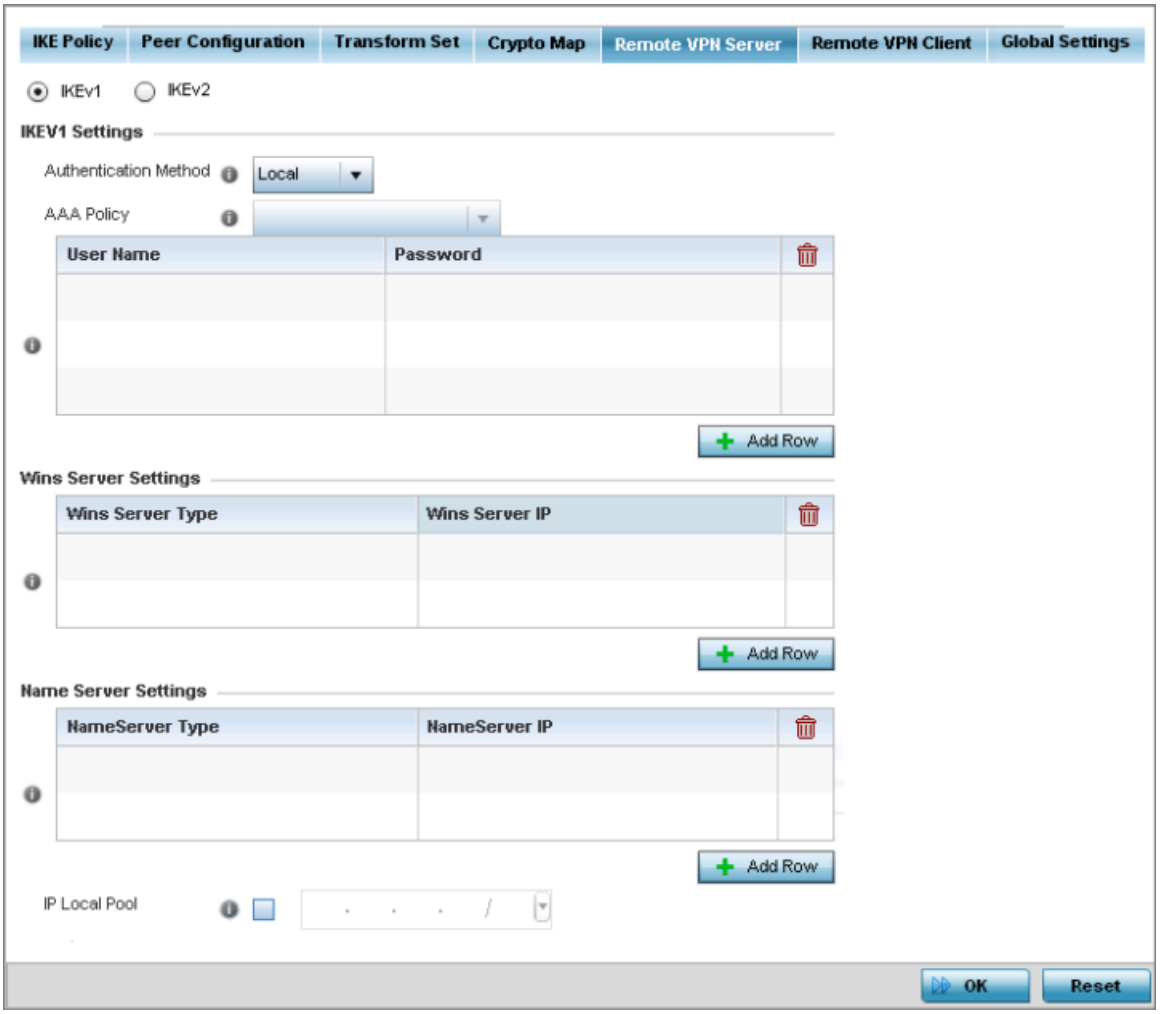



**Figure 87: Profile Security - Remote VPN Server tab (IKEv2 example)**

2 Select either the **IKEv1** or **IKEv2** radio button to enforce peer key exchanges over the remote VPN server using either IKEv1 or IKEv2.

IKEv2 provides improvements from the original IKEv1 design (improved cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.) and is recommended in most deployments. The appearance of the screen differs depending on the selected IKE mode.

3 Set the following IKEv1 or IKe v2 Settings:

| | |
|---|---|
| Authentication Method | Use the drop-down menu to specify the authentication method used to validate the credentials of the remote VPN client. Options include **Local** (on board RADIUS resource if supported) and **RADIUS** (designated external RADIUS resource). If selecting Local, select the **+ Add Row** button and specify a `User Name` and `Password` for authenticating remote VPN client connections with the local RADIUS resource. If selecting RADIUS, specify an AAA policy providing RADIUS server details. |
| AAA Policy | Select the AAA policy used with the remote VPN client. AAA policies define RADIUS authentication and accounting parameters. The access point can optionally use AAA server resources (when using RADIUS as the authentication method) to provide user database information and user authentication data. |

4 Refer to the Username Password Settings table and specify the username and password for validating RADIUS authentication.

5 Refer to the Wins Server Settings table and specify primary and secondary server resources for validating RADIUS authentication requests on behalf of a remote VPN client. These external WINS server resources are available to validate RADIUS resource requests.

6 Refer to the Name Server Settings table and specify primary and secondary server resources for validating RADIUS authentication requests on behalf of a remote VPN client. These external name server resources are available to validate RADIUS resource requests.

7 Select the **IP Local Pool** option to define an IP address and mask for a virtual IP pool used to IP addresses to remote VPN clients.

8 If using IKEv2 specify following additional settings (required for IKEv2 only):

| | |
|---|---|
| DHCP Server Type | Specify whether the Dynamic Host Configuration Protocol (DHCP) server is specified as an IP address, Hostname (FQDN) or None (a different classification will be defined). DHCP allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside. |
| DHCP Server | Depending on the DHCP server type selected, enter either the numerical IP address, hostname or other (if None is selected as the server type). |
| IP Local Pool | Select this option to define an IP address and mask for a virtual IP pool used to IP addresses to remote VPN clients. |
| Relay Agent IP Address | Select this option to define DHCP relay agent IP address. |

9 Select **OK** to save the updates made to the Remote VPN Server screen.

Selecting **Reset** reverts the screen to its last saved configuration.

### Remote VPN Client Configuration

To configure the remote VPN client settings:

1 Select the **Remote VPN Client** tab.

The Remote VPN Client screen provides options for configuring the remote VPN client.

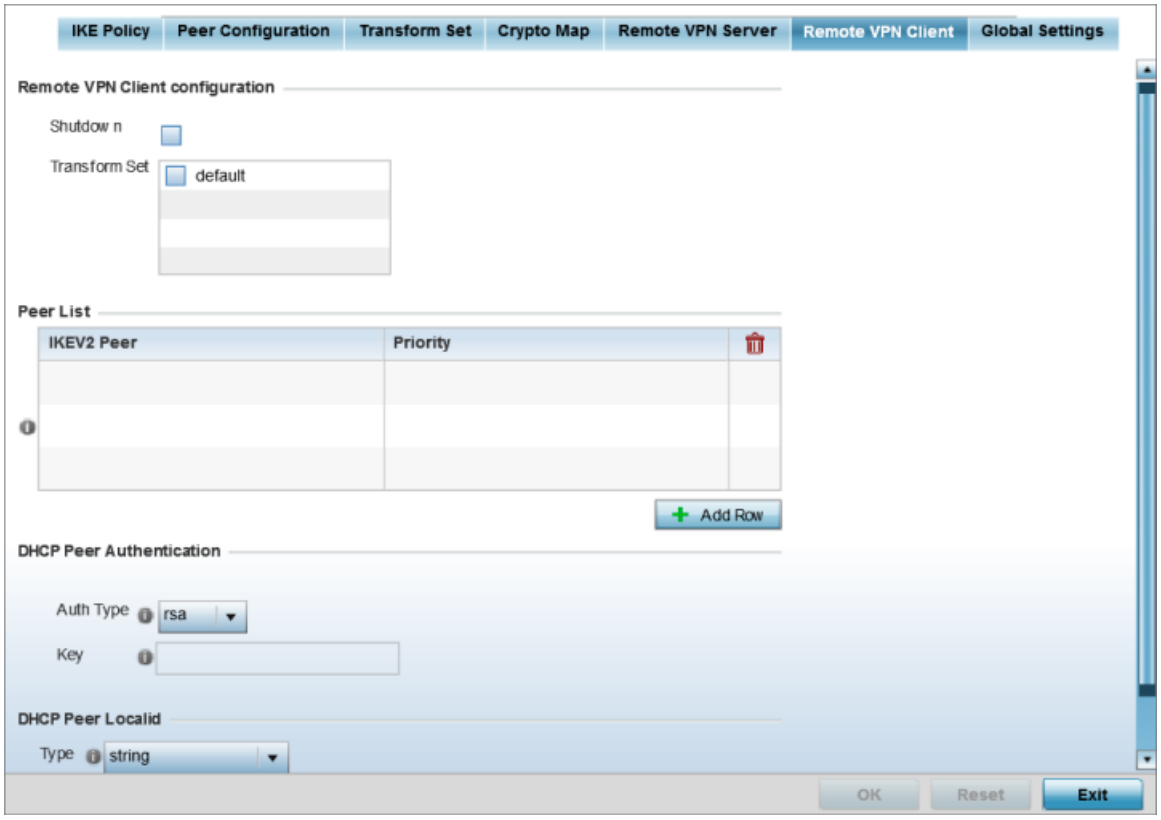



**Figure 88: Profile Security - Remote VPN Client tab**

2 Refer to the following fields to define Remote VPN Client Configuration settings:

| | |
|---|---|
| Shutdown | Select this option to disable the remote VPN client. The default is disabled. |
| Transform Set | Configure the transform set used to specify how traffic is protected within the crypto ACL defining the traffic that needs to be protected. Select the appropriate traffic set from the drop-down menu or click the icon next to the drop-down menu to create a new transform set. |

3 Refer to the following fields to define the Remote VPN Client Peer list:

| | |
|---|---|
| IKEV2 Peer | Use the drop-down menu to select the remote IKE v2 peer. Use the icon next to the drop-down to create a new peer. |
| Priority | Use the spinner to set the priority in which a remote peer is connected. The lower the number the higher the priority. |

4 Set the following DHCP Peer Authentication settings:

| | |
|---|---|
| Auth Type | Use the drop-down menu to specify the DHCP peer authentication type. Options include PSK and RSA. The default setting is RSA. |
| Key | Provide a 8 - 21 character shared key password for DHCP peer authentication. |

5 Set the following DHCP Peer Localid settings:

| | |
|---|---|
| Type | Select the DHCP peer local ID type. Options include string and autogenuniqueid. The default setting is string. |
| Value | Set the DHCP peer local ID. The ID cannot exceed 128 characters. |

6 Select **OK** to save the updates made to the Remote VPN Client screen.

Selecting **Reset** reverts the screen to its last saved configuration.

### Global Settings Configuration

To configure the VPN global settings:

1 Select the **Global Settings** tab.

The Global Settings screen provides options for DPD *(Dead Peer Detection)*. DPD represents the actions taken upon the detection of a dead peer within the IPSec VPN tunnel connection.

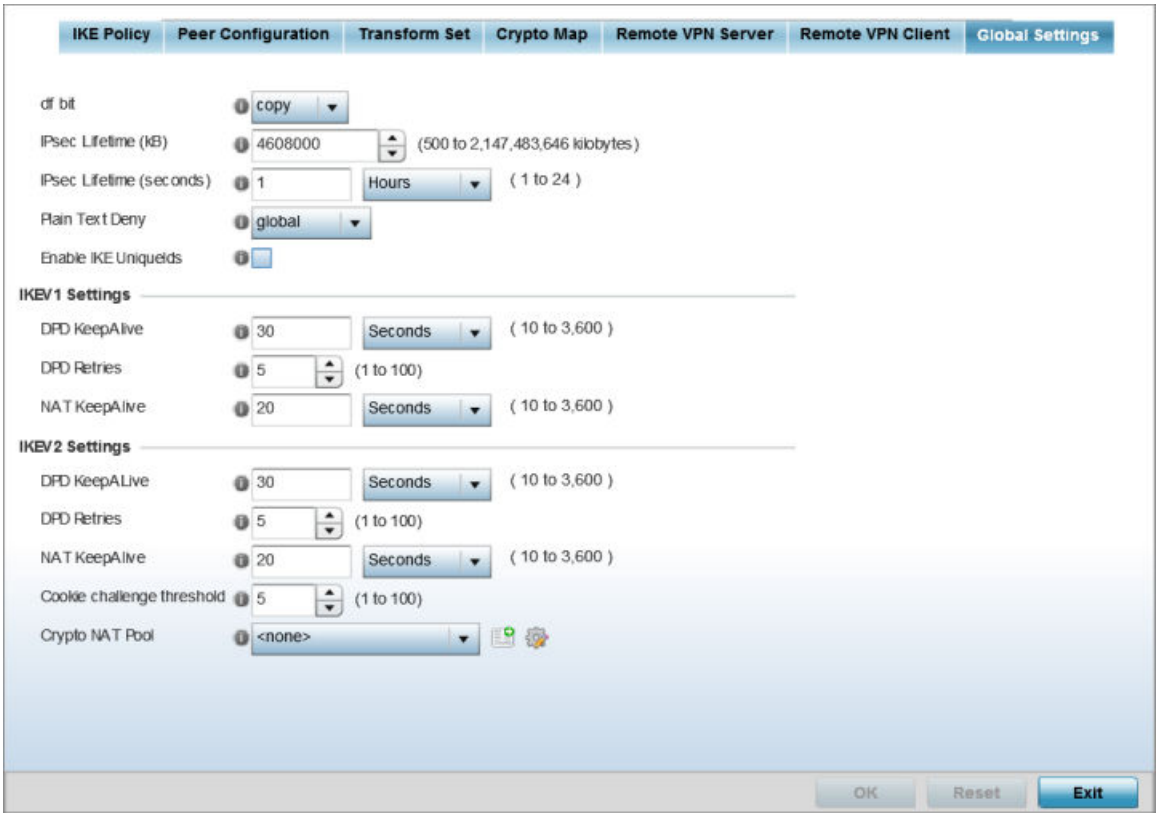



**Figure 89: Profile Security - Global VPN Settings tab**

2 Refer to the following fields to define IPSec security, lifetime and authentication settings:

| | |
|---|---|
| df bit | Select the DF bit handling technique used for the ESP encapsulating header. Options include **clear**, **set** and **copy**. The default setting is copy. |
| IPsec Lifetime (kb) | Set a connection volume lifetime (in kilobytes) for the duration of an IPSec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes. The default settings is 4,608,000 kilobytes. |

| | |
|---|---|
| IPsec Lifetime (seconds) | Set a lifetime (in seconds) for the duration of an IPSec VPN security association. Once the set value is exceeded, the association is timed out. Options include Seconds (120 - 86,400), Minutes (2 - 1,440), Hours (1 - 24) or Days (1). The default setting is 3,600 seconds. |
| Plain Text Deny | Select global or interface to set the scope of the ACL. The default setting is global, expanding the rules of the ACL beyond just the interface. |
| Enable IKE UniqueIds | Select this option to initiate a unique ID check. This is disabled by default. |

3 Define the following IKEv1/IKEv2 DPD settings:

| | |
|---|---|
| DPD Keep Alive | Define the interval (or frequency) of IKE keep alive messages for dead peer detection. Options include Seconds (10 - 3,600), Minutes (1 - 60) and Hours (1). The default setting is 30 seconds. |
| DPD Retries | Use the spinner control to define the number of keep alive messages sent to an IPSec VPN client before the tunnel connection is defined as dead. The available range is from 1 - 100. The default number of messages is 5. |
| NAT Keep Alive | Define the interval (or frequency) of NAT keep alive messages for dead peer detection. Options include Seconds (10 - 3,600), Minutes (1 - 60) and Hours (1). The default setting is 20 seconds. |
| Cookie Challenge Threshold | Use the spinner control to define the threshold (1 - 100) that, when exceeded, enables the cookie challenge mechanism. |
| Crypto NAT Pool | Use the drop-down menu to select the NAT pool for internal source NAT for IPSec tunnels. |

4 Select **OK** to save the updates made to the Global Settings screen.

Selecting **Reset** reverts the screen to its last saved configuration.

### *Defining Profile Auto IPSec Tunnel Settings*

IPSec tunnels are established to secure traffic, data and management traffic, from access points to remote wireless controllers. Secure tunnels must be established between access points and the wireless controller with minimum configuration pushed through DHCP option settings.

Note

WiNG 7.1 release is not supported on AP505i and AP510i model access points. This feature will be supported in future releases,

To define or override a profile's Auto IPSec tunnel configuration:

1 Select **Configuration** > **Devices** > **System Profile** from the web UI.

2 Expand the **Security** menu and select **Auto IPSec Tunnel**.

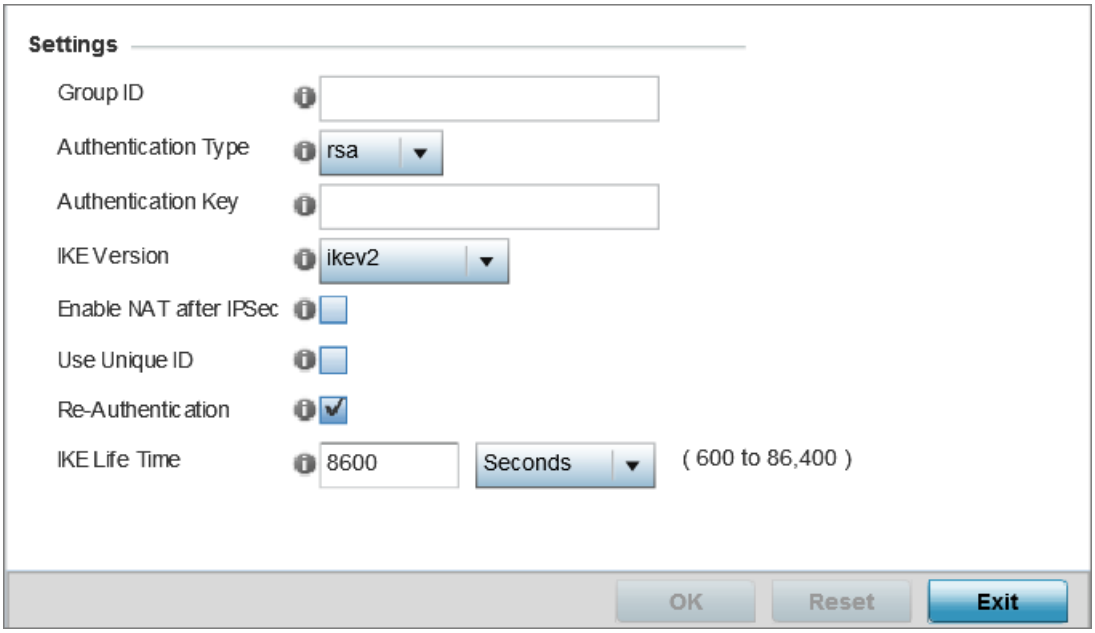



**Figure 90: Profile Security - Auto IPSec Tunnel Screen**

3 Refer to the following table to configure the Auto IPSec Tunnel settings:

| | |
|---|---|
| Group ID | Configure the ID string used for IKE authentication. String length can be between 1 and 64 characters. |
| Authentication Type | Set the IPSec Authentication Type. Options include **PSK** (Pre Shared Key) or **RSA**. |
| Authentication Key | Set the common key for authentication between the remote tunnel peer. Key length is between 8 and 21 characters |
| IKE Version | Configure the IKE version to use. The available options are **ikev1-main**, **ikev1- aggr** and **ikev2**. |
| Enable NAT after IPSec | Select this option to enable NAT after IPSec. Enable this if there are NATted networks behind VPN tunnels. |
| Use Unique ID | In scenarios where different access points behind different NAT boxes and routers have the same IP address, it is not possible to create a tunnel between the wireless controller and the access point because the wireless controller does not identify the access point uniquely. When this option is selected, each access point behind a same NAT box or router will have an unique ID which is used to create the VPN tunnel. |
| Re-Authentication | Select this option to re-authenticate the key on a IKE rekey. This setting is disabled by default. |
| IKE Life Time | Set a lifetime in either seconds (600 - 86,400), minutes (10 - 1,440), hours (1 - 24), or days (1) for IKE security association duration. The default setting is 8600 seconds. |

4 Click **OK** to save the changes made in the Auto IPSec Tunnel screen.

Click **Reset** to revert to the last saved configuration.

*Defining Profile Security Settings*

A profile can make use of existing firewall, wireless client role, and WIPS policies and apply them to the profile's configuration. This affords each profile a truly unique combination of data protection policies

for best meeting the data protection requirements of the profile it supports. However, as deployment requirements arise, an individual device may need some or all of its general security configuration overridden from the profile's settings.

To configure a profile's security settings and overrides:

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Security** menu and select **Settings**.

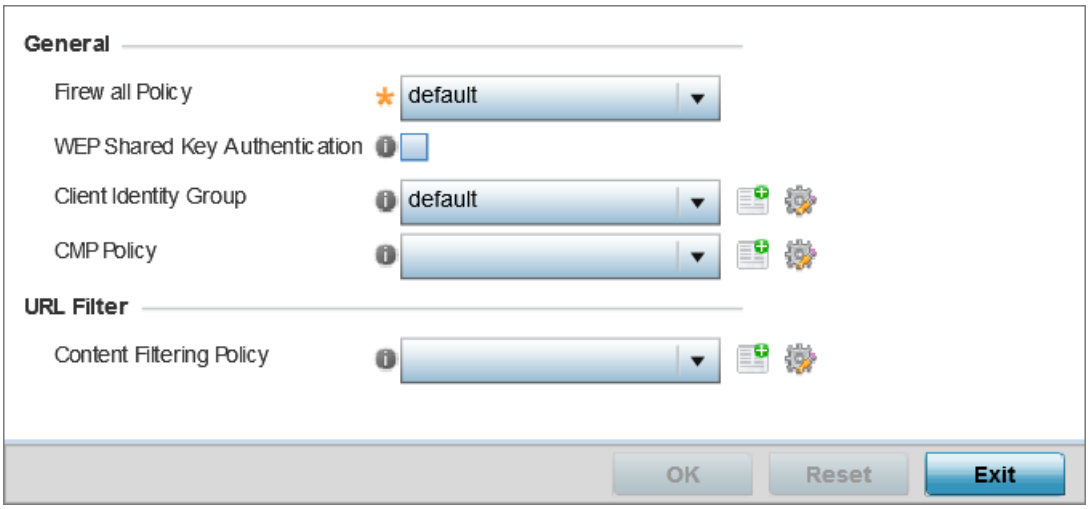



**Figure 91: Profile Security - Settings screen**

3 Select a firewall policy from the **Firewall Policy** drop-down menu. All devices using this profile must meet the requirements of the firewall policy to access the network. A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic within the network. If an existing Firewall policy does not meet your requirements, select the Create icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and edited as needed using the Edit icon.

4 Select the **WEP Shared Key Authentication** option to require profile supported devices to use a WEP key to access the network using this profile. The access point, other proprietary routers, and our clients use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without our adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

5 Client Identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for devices classes in the network. A client identity group is a collection of client identities that identify devices and applies specific permissions and restrictions on these devices. From the drop-down menu select the **Client Identity Group** to use with this device profile. For more information, see Device Fingerprinting on page 762.

6 Use the CMP Policy drop-down menu to apply a CMP policy. CMP *(Certificate Management Protocol)* is an Internet protocol to obtain and manage digital certificates in a PKI *(Public Key Infrastructure)* network. A CA *(Certificate Authority)* issues the certificates using the defined CMP.

7 Use the **URL Filter** drop-down menu to select or override the URL Filter configuration applied to this virtual interface.

URL filtering is used to restrict access to resources on the internet.

8 Click **OK** to save the changes or overrides.

Click **Reset** to revert to the last saved configuration.

### *Setting the Certificate Revocation List (CRL) Configuration*

A CRL *(certificate revocation list)* is a list of revoked certificates that are no longer valid. A certificate can be revoked if the CA *(certificate authority)* has improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is that the user is no longer in sole possession of the private key.

To define a certificate revocation configuration or override:

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Security** menu and select **Certificate Revocation**.

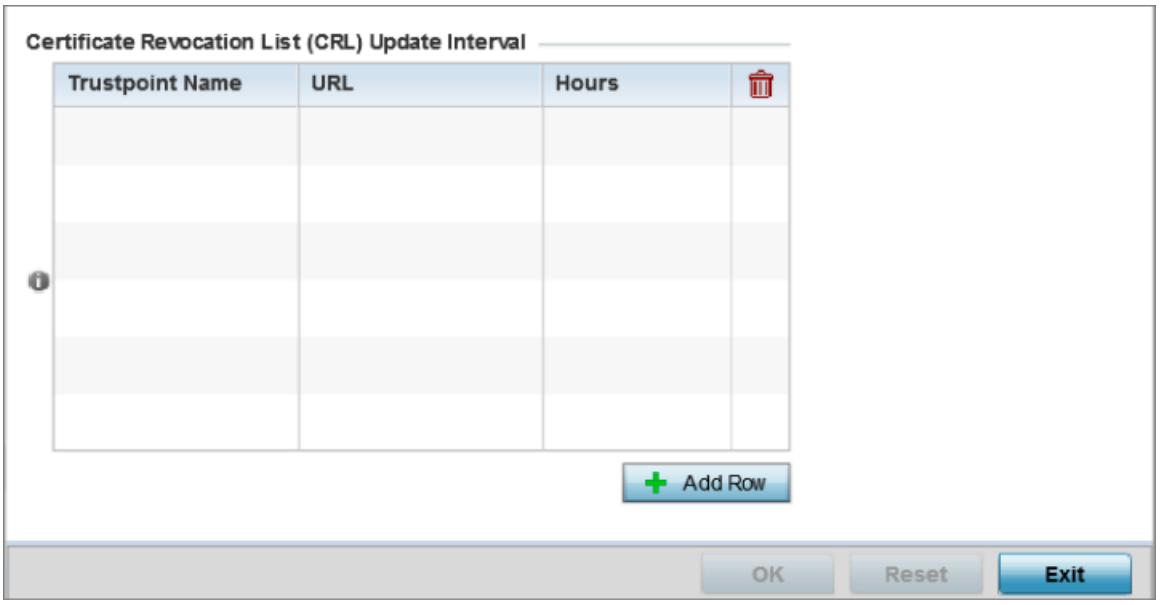



**Figure 92: Profile Security - Certificate Revocation List (CRL) Update Interval Screen**

3 Click **+ Add Row**, in the Certificate Revocation List (CRL) Update Interval table to quarantine certificates from use in the network.

Additionally, a certificate can be placed on hold for a user defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.

a In the Trustpoint Name field, provide the name of the trustpoint in question.

The name cannot exceed 32 characters.

b In the URL field, enter the third-party resource ensuring the trustpoint's legitimacy.

c Use the spinner control to specify an interval (in hours) after which a device copies a CRL file from an external server and associates it with a trustpoint.

4 Click **OK** to save the changes or overrides to the Certificate Revocation screen.

Click **Reset** to revert to the last saved configuration.

*Setting the RADIUS Trustpoint Configuration*

A RADIUS certificate links identity information with a public key enclosed in the certificate. A CA *(certificate authority)* is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.

To define a RADIUS Trustpoint configuration, utilize an existing stored trustpoint or launch the certificate manager to create a new one:

1 Select **Configuration → Devices → System Profiles** from the web UI.

The Profile screen displays. This screen displays a list of profiles.

2 Select a profile from those listed.

The selected profile's configuration menu displays.

3 Expand the **Security** menu and select **Trustpoints**.

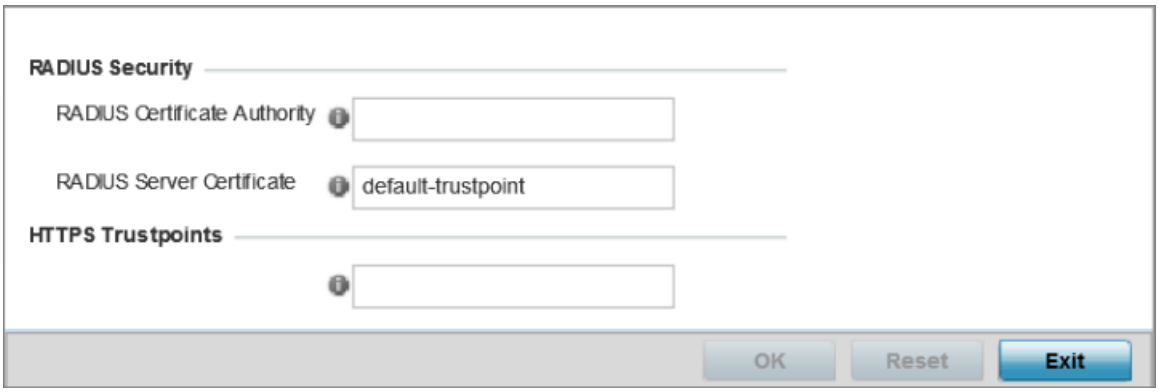



**Figure 93: Security - RADIUS Truspoint screen**

4 Set the following **RADIUS Security** certificate settings:

| | |
|---|---|
| RADIUS Certificate Authority | Either use the default-trustpoint or select the **Stored** radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the **Launch Manager** button. |
| RADIUS Server Certificate | Either use the default-trustpoint or select the **Stored** radio button to enable a drop-down menu where an existing certificate/trustpoint can be used. To leverage an existing trustpoint, select the **Launch Manager** button. |

5 Set the following HTTPS Trustpoints certificate settings:

| | |
|---|---|
| HTTPS Trustpoint | Either use the **`default-trustpoint`** or click **Stored** to enable a drop-down menu where an existing certificate/trustpoint can be used. To use an existing certificate for this device, click **Launch Manager**. For more information, see Certificate Management on page 891. |

6 Click **OK** to save the changes made in the RADIUS Trustpoints screen.

Click **Reset** to revert to the last saved configuration.

*Setting the NAT Configuration*

NAT *(Network Address Translation)* is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller, service platform or access point managed network address credentials. With typical deployments, NAT

is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

Additionally, NAT is a process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping one IP address to another. In most deployments NAT is used in conjunction with IP masquerading which hides RFC1918 private IP addresses behind a single public IP address.

NAT can provide a profile outbound internet access to wired and wireless hosts connected to a controller, service platform or access point. Many-to-one NAT is the most common NAT technique for outbound internet access. Many-to-one NAT allows a controller, service platform or access point to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Security** menu and select **NAT**.

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the Basic Configuration section of the device and click **Clear Overrides**. This removes all overrides from the device.

The NAT Pool screen displays by default. The NAT Pool screen lists the NAT policies that have been created thus far. Any of these policies can be selected and applied to a profile.

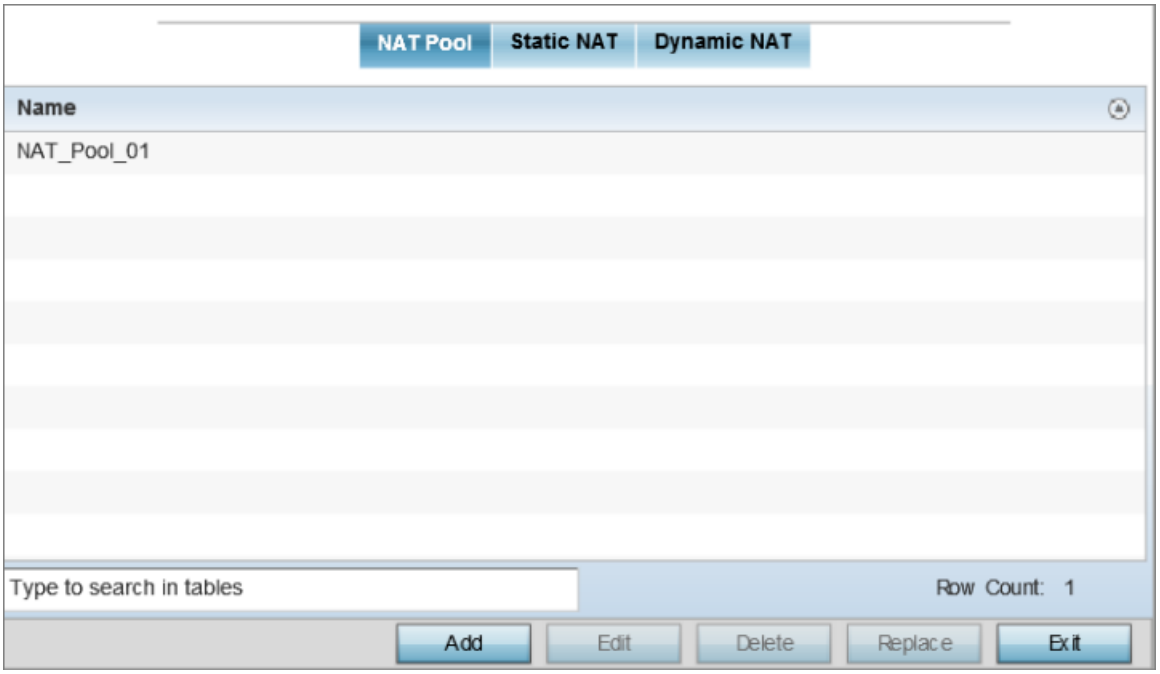



**Figure 94: Profile Security - NAT Pool tab**

3 Review the existing NAT Pool configurations.

### Adding Editing NAT Pool Configuration

1 Click **+ Add Row**, in the IP Address Range table to append additional rows.

Click **Edit** to modify or override the attributes of a existing policy, or click **Delete** to remove obsolete NAT policies from the list of those available to a profile.

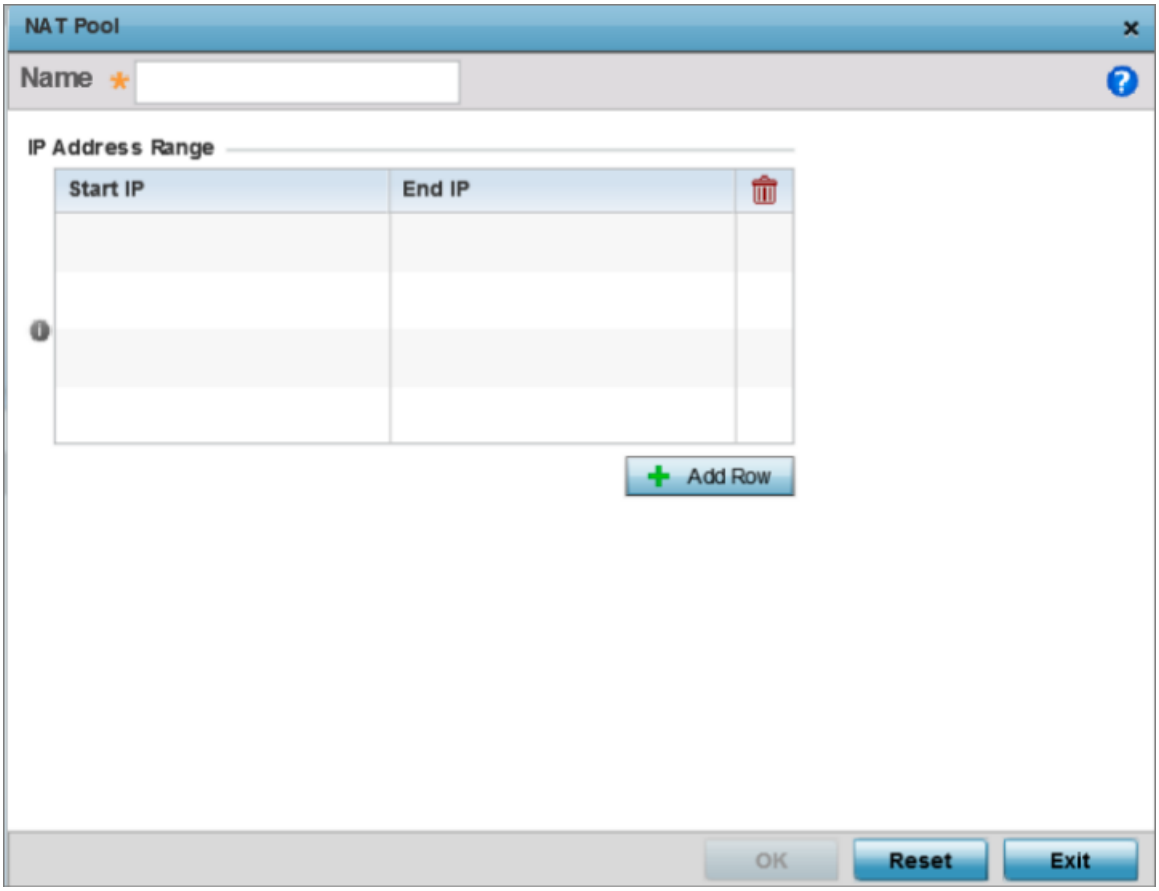



**Figure 95: Profile Security - NAT Pool tab - NAT Pool field**

2 If you are adding a new NAT policy, provide a **Name** to help distinguish it from others with similar configurations. The length cannot exceed 64 characters.

3 Click **+ Add Row**, in the IP Address Range table to append additional rows.

| | |
|---|---|
| Sart IP - End IP | Define a range of IP addresses that are hidden from the public internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from potentially being routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall. |

4 Click **OK** to save the changes made to the profile's NAT pool configuration.

Click **Reset** to revert to the last saved configuration.

### Static NAT Source Configuration

*Static* NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a web server on a perimeter interface with the internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized

users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

To add or edit a Static NAT source configuration:

1 Select the **Static NAT** tab.

The Source tab displays by default and lists existing static NAT configurations. Existing static NAT configurations are not editable, but new configurations can be added or existing ones deleted as they become obsolete.

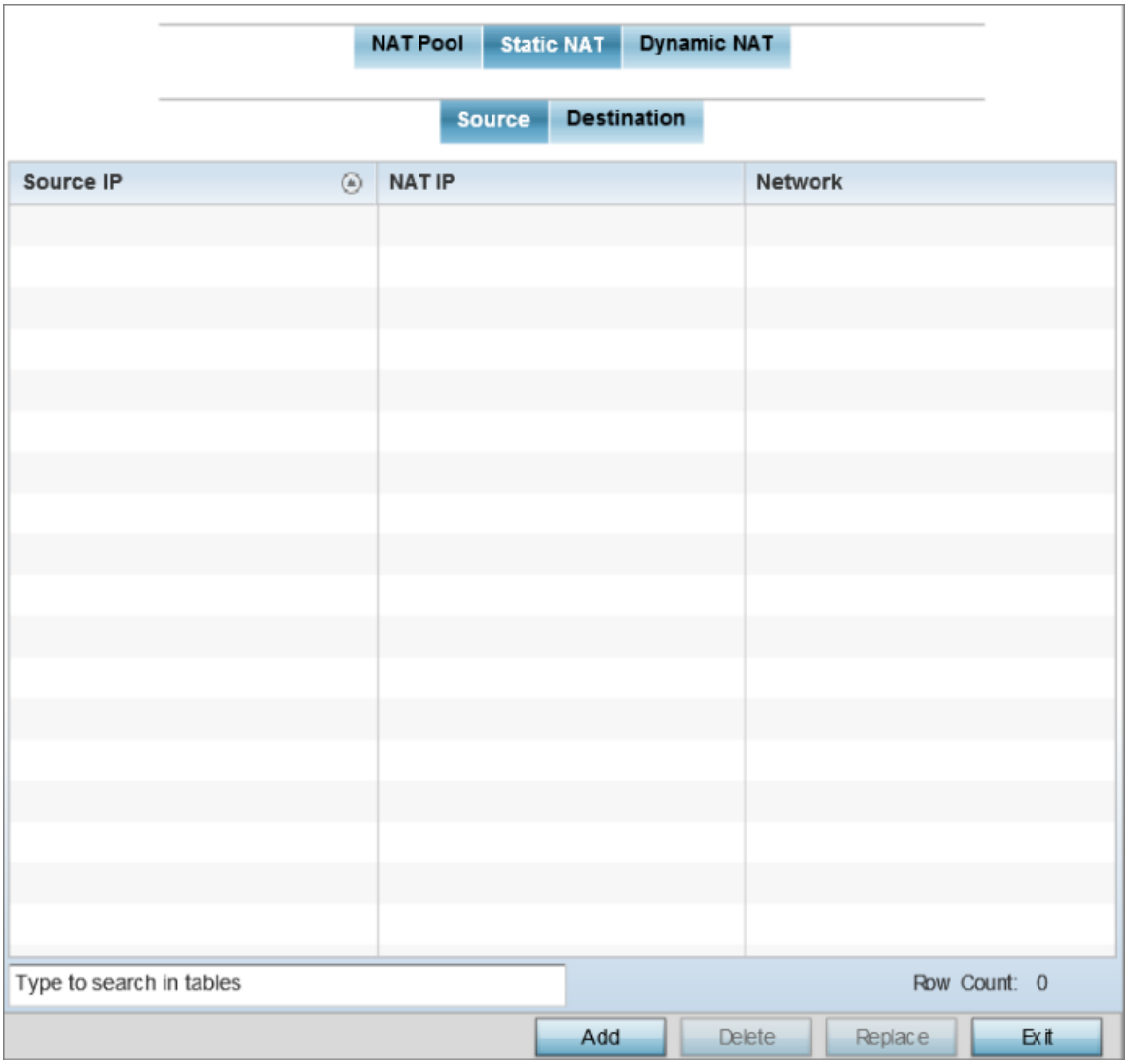



**Figure 96: Profile Security - Static NAT screen - Source tab**

2 To map a source IP address from an internal network to a NAT IP address, click **Add**.

3 Define the following Source NAT parameters:

| | |
|---|---|
| Source IP | Enter the address used at the (internal) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination. |
| NAT IP | Enter the IP address of the matching packet to the specified value. The IP address modified can be either **`source`** or **`destination`** based on the direction specified. |
| Network | Select **`Inside`** or **`Outside`** NAT as the network direction. The default setting is Inside.<br>Select *Inside* to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a web server on a perimeter interface with the internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host. |

4 Click **OK** to save the changes made to the Static NAT Source configuration.

Click **Reset** to revert to the last saved configuration.

### Static NAT Destination Configuration

NAT destination configurations define the way in which packets passing through the NAT on the way back to the LAN are searched against the records kept by the NAT engine. The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the network.

To add or edit a Static NAT destination configuration:

1 Select the **Destination** tab.

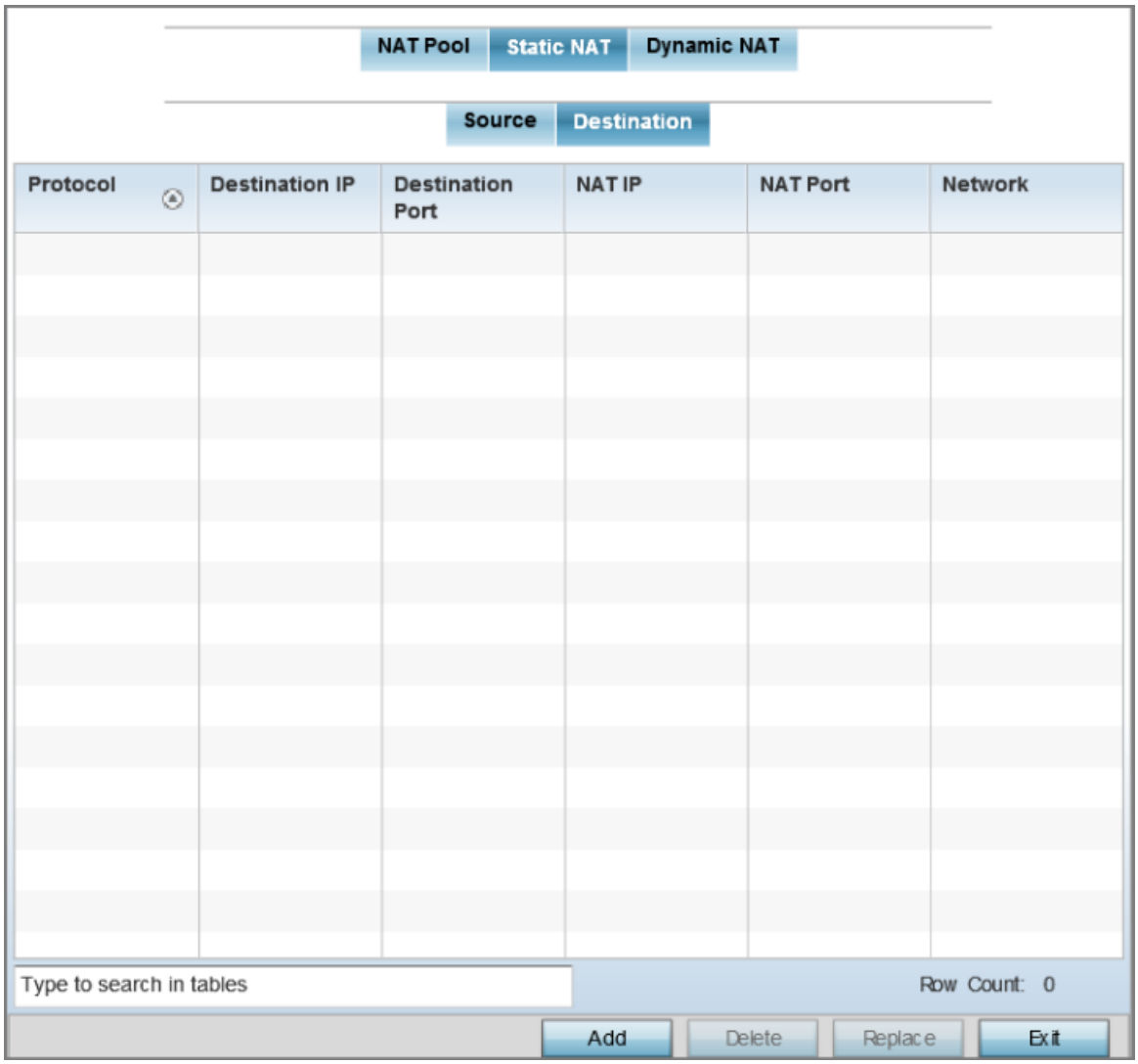
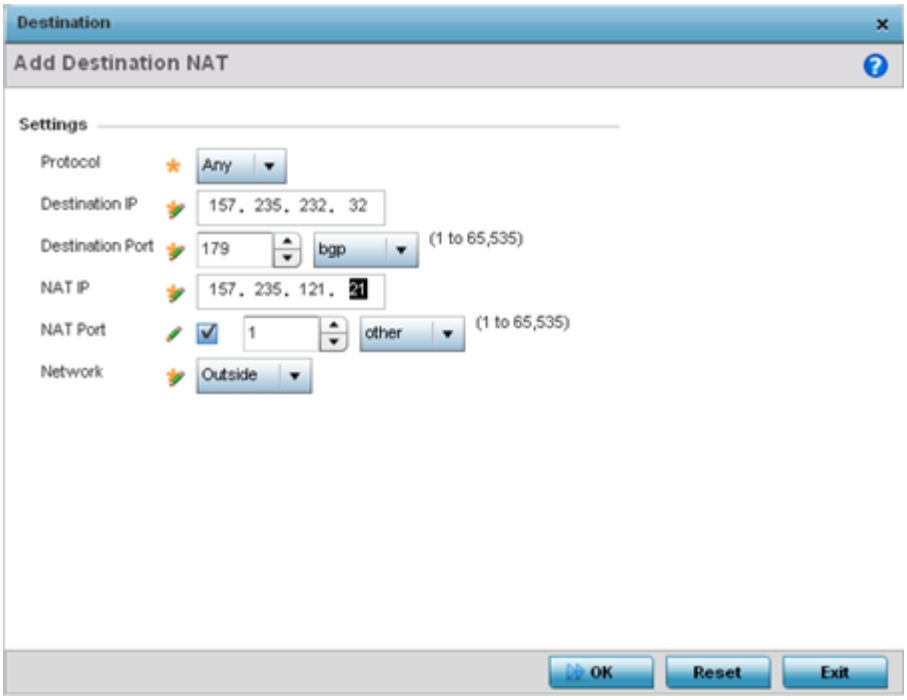



**Figure 97: Profile Security - Static NAT screen - Destination tab**

2 Review existing Static NAT destination configurations to determine if a new configuration warrants creation or an existing configuration warrants modification or deletion.

3 Select **Add** to create a new NAT destination configuration, **Edit** to modify the attributes of an existing configuration or **Delete** to permanently remove a NAT destination.




4 Set the following Destination configuration parameters:

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and an external network. To share a Web server with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual server address from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

| | |
|---|---|
| Protocol | Select the protocol for use with static translation. *TCP, UDP* and *Any* are available options. TCP is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The *User Datagram Protocol* (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is Any. |
| Destination IP | Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) is not be exposed to the outside world when the translation address is used to interact with the remote destination. |
| Destination Port | Use the spinner control to set the local port used at the (source) end of the static NAT configuration. The default port is 1. |
| NAT IP | Enter the IP address of the matching packet to the specified value. The IP address modified can be either *source* or *destination* based on the direction specified. |
| NAT Port | Set the port number of the matching packet to the specified value. This option is valid only if the direction specified is destination. |
| Network | Select *Inside* or *Outside* NAT as the network direction. Inside is the default setting. |

5 Click **OK** to save the changes made to the static NAT configuration.

ion. Select **Reset** to revert to the last saved configuration.

### Dynamic NAT Configuration

Dynamic NAT configurations translate the IP address of packets going out from one interface to another interface based on configured conditions. Dynamic NAT requires packets be switched through a NAT router to generate translations in the translation table.

To add or edit dynamic NAT settings:

1 Select the **Dynamic NAT** tab.

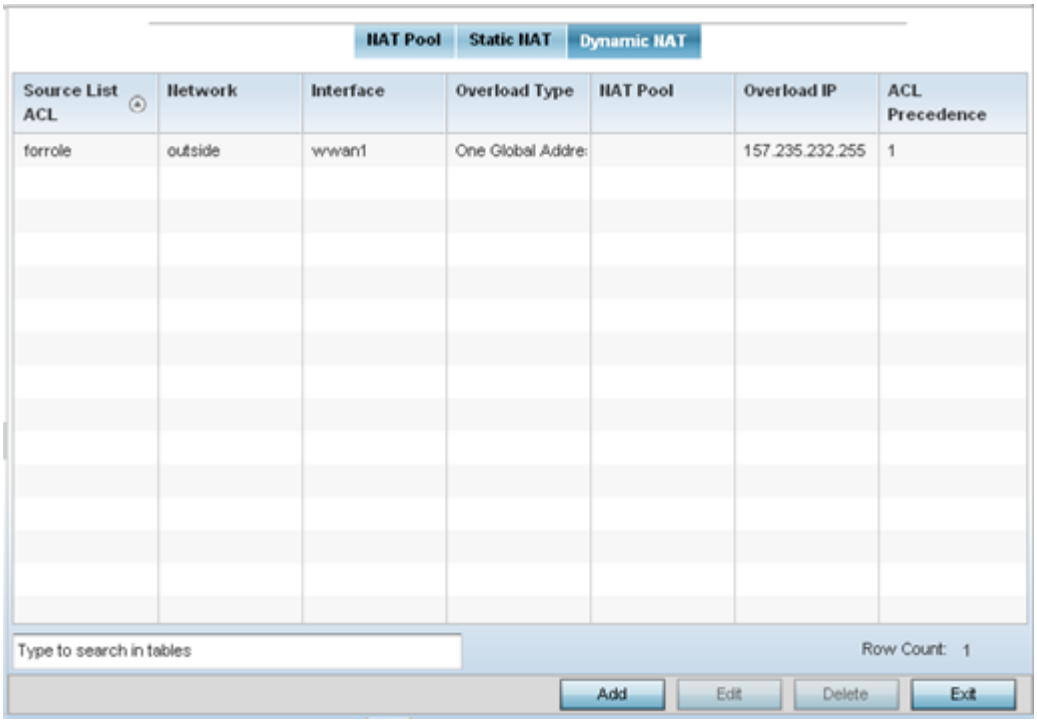



**Figure 98: Profile Security - Dynamic NAT tab**

2 Refer to the following to determine whether a new dynamic NAT configuration needs to be created, or whether an existing one can be edited or deleted:

| | |
|---|---|
| Source List ACL | Lists an ACL to define the packet selection criteria for the NAT configuration. NAT is applied only on packets which match a rule defined in the access-list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination. |
| Network | Displays **Inside** or **Outside** NAT as the network direction for the dynamic NAT configuration. |
| ACL Precedence | Lists the administrator-assigned priority set for the listed source list ACL. The lower the value listed, the higher the priority assigned to this ACL rule. |
| Interface | Lists the VLAN (from 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. |

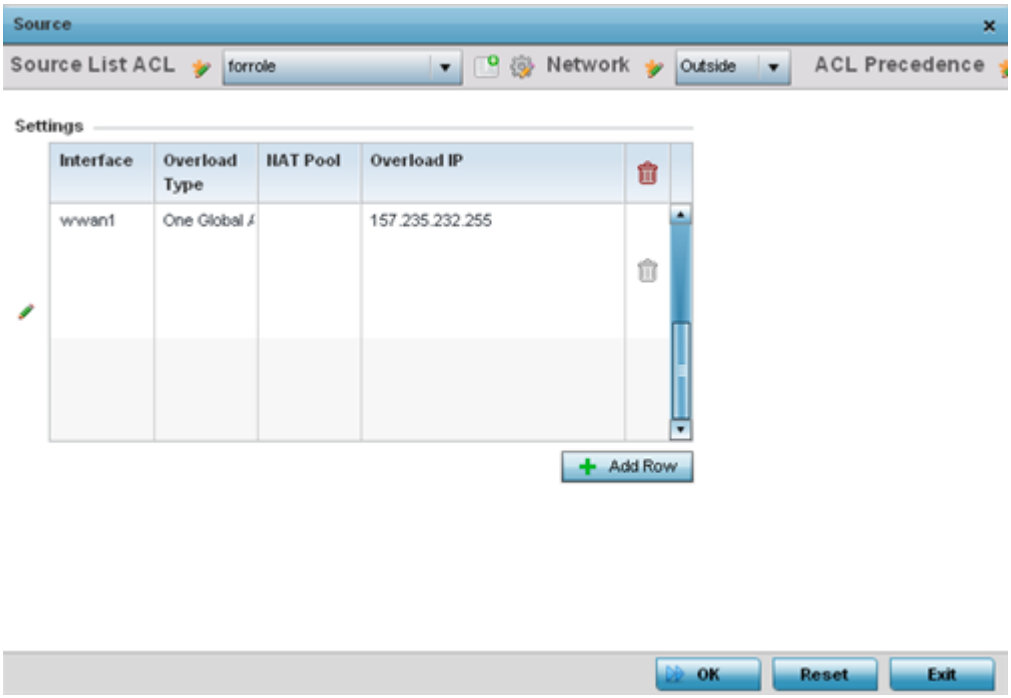
| | |
|---|---|
| Overload Type | Displays the overload type used when several internal addresses are NATed to only one or a few external addresses. Options include **`NAT Pool`**, **`One Global Address`** and **`Interface IP Address`**. The default setting is Interface IP Address. |
| NAT Pool | Displays the name of an existing NAT pool used with the dynamic NAT configuration. |
| Overload IP | If **`One Global IP Address`** is selected as the **Overload Type**, define an IP address to use as a filter address for the IP ACL rule. |

3 To modify an existing dynamic NAT configuration, select it and click **Edit**. To remove an existing configuration, select it and click **Delete**.

Adding and Editing Dynamic NAT

To add or edit a dynamic NAT configuration that can be applied to a profile:

1 Select Add to create a new Dynamic NAT configuration, Edit to modify an existing configuration or Delete to permanently remove a configuration.




2 Set the following to define the Dynamic NAT configuration:

| | |
|---|---|
| Source List ACL | Use the drop-down menu to select an ACL name to define the packet selection criteria for NAT. NAT is applied only on packets which match a rule defined in the access list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination. |
| Network | Select *Inside* or *Outside* NAT as the network direction for the dynamic NAT configuration. Inside is the default setting. |
| ACL Precedence | Set the priority (from 1 - 5000) for the source list ACL. The lower the value, the higher the priority assigned to these ACL rules. |

| | |
|---|---|
| Interface | Use the drop-down menu to select the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected represents the intended network traffic within the NAT supported configuration. VLAN1 is available by default. |
| Overload Type | Select the check box of Overload Type used with the listed IP ACL rule. Options include *NAT Pool*, *One Global Address* and *Interface IP Address*. Interface IP Address is the default setting. |
| NAT Pool | Provide the name of an existing NAT pool for use with the dynamic NAT configuration. |
| Overload IP | Enables the use of one global address for numerous local addresses. |

3 Select OK to save the changes made to the dynamic NAT configuration. Select Reset to revert to the last saved configuration.

### *Bridge NAT Configuration*

Use Bridge NAT to manage Internet traffic originating at a remote site. In addition to traditional NAT functionality, Bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router.

Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

Note
Bridge NAT supports single AP deployments only. This feature cannot be used in a branch deployment with multiple access points.

To define a Bridge NAT configuration that can be applied to a profile:

1 Select **Configuration → Devices → System Profile** from the web UI.

2 Expand the **Security** menu and select **Bridge NAT**.

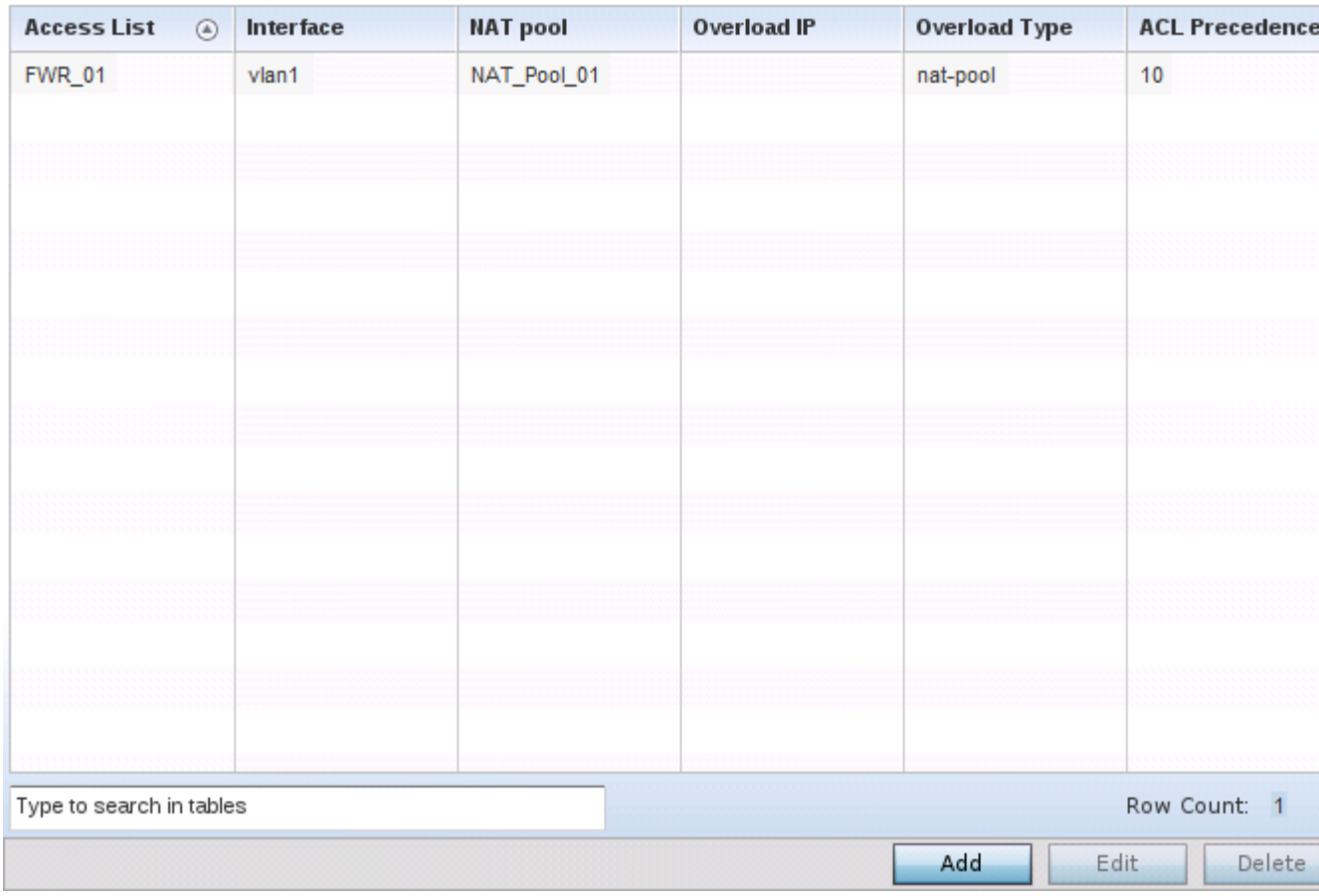



**Figure 99: Profile Security - Bridge NAT Screen**

3 Review the following Bridge NAT configurations to determine whether a new Bridge NAT configuration requires creation or an existing configuration modified or removed.

| | |
|---|---|
| Access List | Lists the ACL applying IP address *access/deny* permission rules to the Bridge NAT configuration. |
| Interface | Lists the communication medium (outgoing layer 3 interface) between source and destination points. This is either the access point's **`pppoe1`** or **`wwan1`** interface or the VLAN used as the redirection interface between the source and destination. |
| NAT Pool | Lists the names of existing NAT pools used with the Bridge NAT configuration. This displays only when *Overload Type* is NAT Pool. |
| Overload IP | Lists the IP address used globally for numerous local addresses. |
| Overload Type | Lists the overload type used with the listed IP ACL rule. Set as either **`NAT Pool`**, **`One Global Address`** or **`Interface IP Address`**. |
| ACL Precedence | Lists the administrator assigned priority set for the ACL. The lower the value listed the higher the priority assigned to these ACL rules. |

### Adding and Editing Bridge NAT Configuration

1 Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

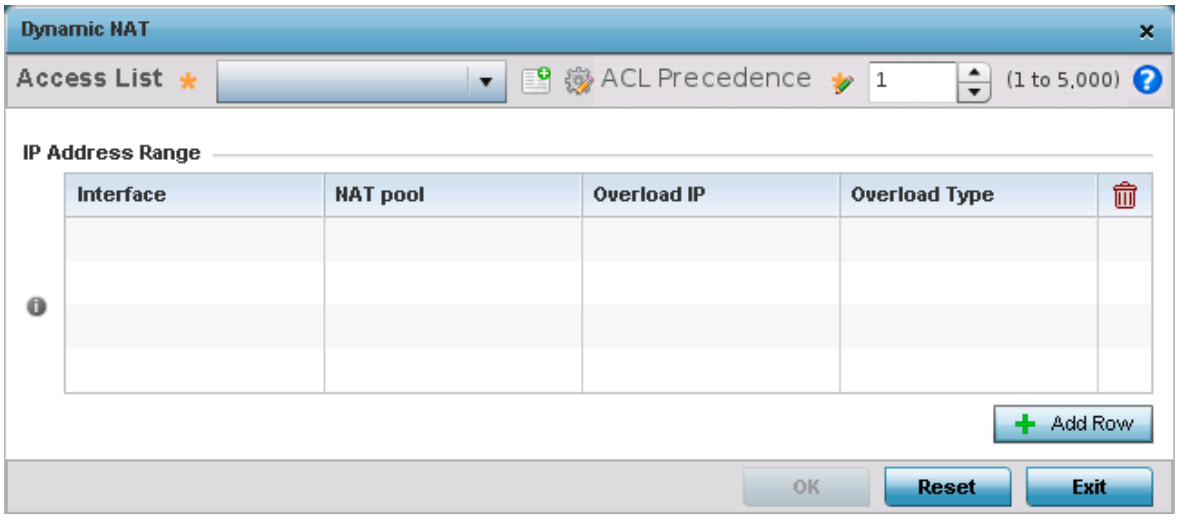



**Figure 100: Profile Security - Dynamic NAT screen**

2 Select the **ACL** whose IP rules are to be applied to this policy based forwarding rule. A new ACL can be defined by selecting the **Create** icon, or an existing set of IP ACL rules can be modified by selecting the **Edit** icon.

3 Use the IP Address Range table to configure IP addresses and address ranges that can used to access the Internet.

| | |
|---|---|
| Interface | Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an access point WWAN or PPPoE interface. Traffic can also be redirected to a designated VLAN. |
| NAT Pool | Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to NAT Pool. |
| Overload IP | Lists the IP address used to represent a large number local addresses for this configuration. |
| Overload Type | Displays the override type for this policy based forwarding rule. |

4 Select **+ Add Row** to set the IP Address Range settings for the Bridge NAT configuration.

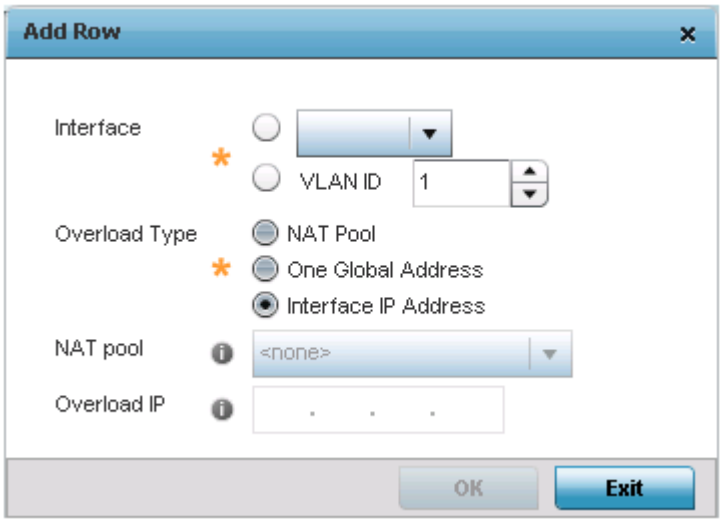



**Figure 101: Profile Security - Source Dynamic NAT screen - Add Row field**

5 Select **OK** to save the changes made within the Add Row and Dynamic NAT screens. Select **Reset** to revert to the last saved configuration.

## *Defining Profile Application Visibility Settings*

*Deep packet inspection* (DPI) is an advanced packet filtering technique functioning at the application layer. Use DPI to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the WiNG managed network. The contents of each packet are scanned, occasionally logged and blocked or routed to their destination. Deep packet inspection helps an ISP block the spread of viruses, illegal downloads and prioritize data transmitted by bandwidth-heavy applications (video and VoIP applications) to help prevent network congestion.

DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When DPI is enabled, packets of all flows are subjected to DPI to get accurate results. DPI identifies applications (such as, Netflix, Twitter, Facebook, etc.) and extracts metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

Note
The WiNG 7.1 release does not provide DPI support on AP505 and AP510 model access points. This feature will be supported in future releases.

To configure a profile's application visibility settings and overrides:

1 Go to **Configuration → Devices → System Profiles** .

2 Expand the **Security** menu and select **Application Visibility (AVC)**.

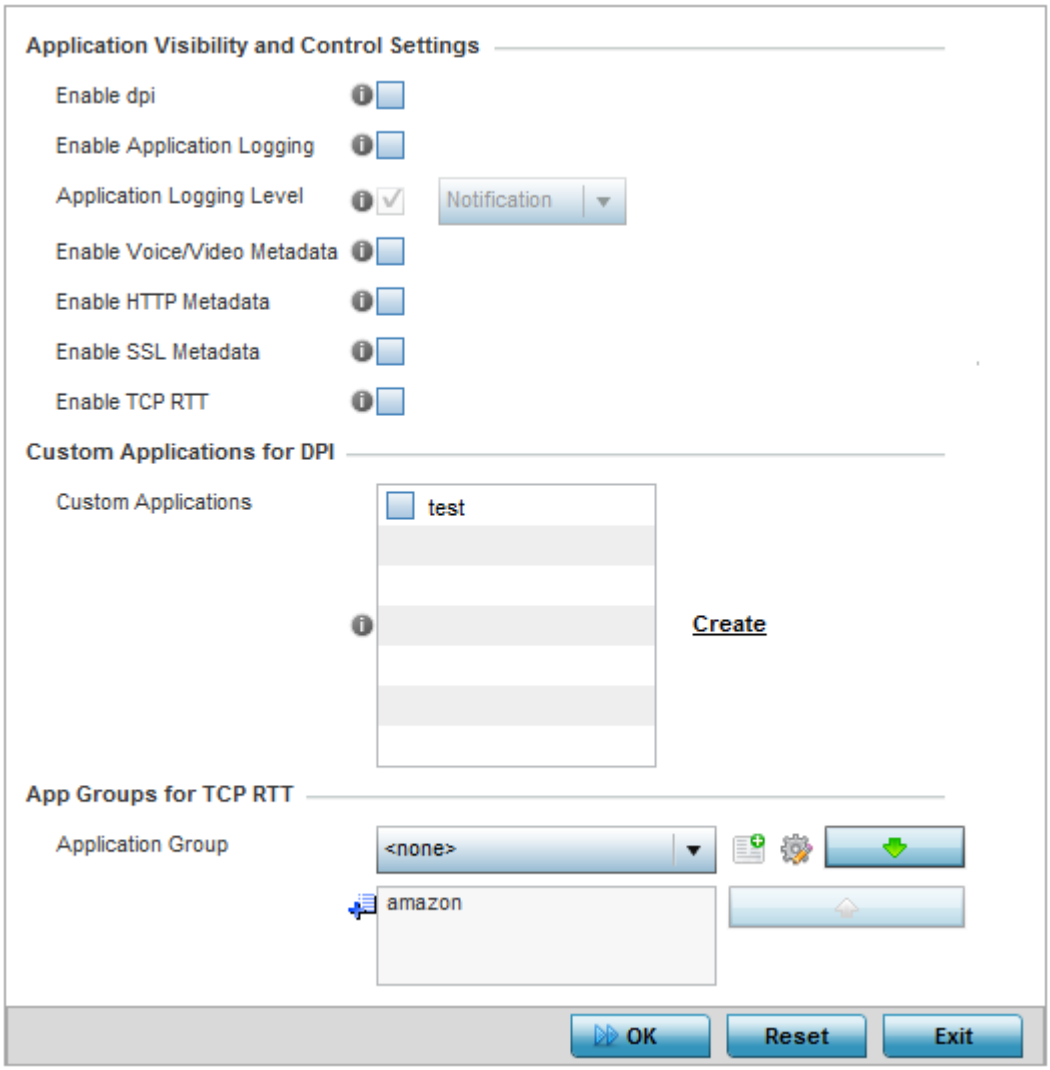



**Figure 102: Profile Security - Application Visibility Screen**

3 Refer the following Application Visibility and Control settings:

| | |
|---|---|
| Enable dpi | Enable this setting to provide deep-packet inspection (application assurance) by inspecting every byte of each application header packet passing through the controller or service platform. When enabled, application data streams are inspected at a granular level to help prevent viruses and spyware from accessing the WiNG managed network. |
| Enable Applications Logging | Select this option to enable event logging for DPI application recognition. This setting is disabled by default. |
| Applications Logging Level | If enabling DPI application recognition event logging, set the logging level. Severity levels include **Emergency**, **Alert**, **Critical**, **Errors**, **Warning**, **Notice**, **Info**, and **Debug**. The default logging level is Notification. |
| Enable Voice/Video Metadata | Select this option to enable the metadata extraction from voice and video classified flows. The default setting is disabled. |

| | |
|---|---|
| Enable HTTP Metadata | Select this option to enable extraction of metadata from HTTP application data flows. The default setting is disabled. |
| Enable SSL Metadata | Select this option to enable extraction of metadata from SSL application data flows. The default setting is disabled. |
| Enable TCP RTT | Select this option to enable extraction of RTT information from TCP flows. The default setting is disabled. |

4 Review the Custom Applications for DPI field to select the custom applications available for this device profile.

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

Click **Reset** to revert to the last saved configuration.

## Virtual Router Redundancy Protocol

A default gateway is a critical resource for connectivity. However, it's prone to a single point of failure. Thus, redundancy for the default gateway is required by the access point. If WAN backhaul is available, and a router failure occurs, then an access point should act as a router and forward traffic on to its WAN link.

Define an external VRRP *(Virtual Router Redundancy Protocol)* configuration when router redundancy is required in a wireless network requiring high availability.

The election of a VRRP master is central to the configuration of VRRP. A VRRP master (once elected) performs the following functions:

- Responds to ARP requests
- Forwards packets with a destination link layer MAC address equal to the virtual router MAC address
- Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner
- Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true

Nodes that lose the election process enter a backup state where they monitor the master for any failures. In case of a failure, one of the backups becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.

To define the configuration of a VRRP group:

1 Select the **Configuration → Devices → System Profile → VRRP** tab from the web UI.

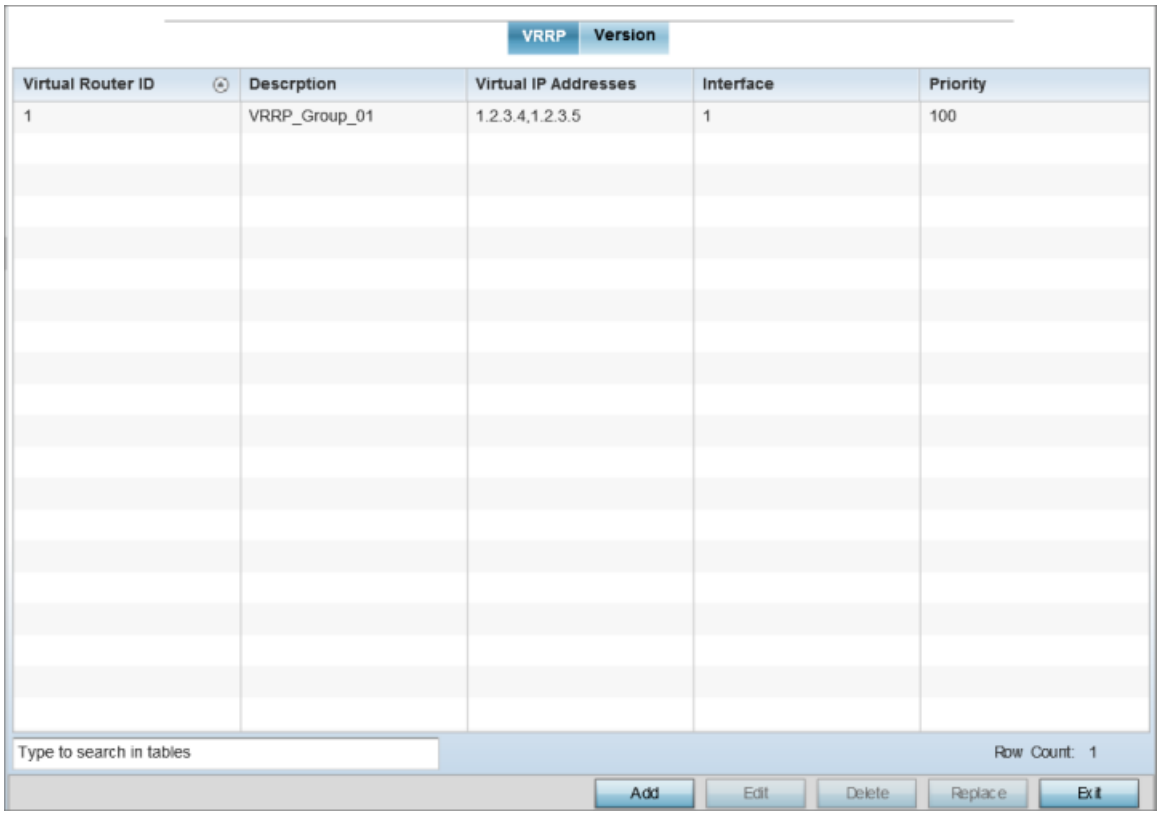



**Figure 103: Profiles - VRRP screen - VRRP tab**

2 Review the following VRRP configuration data to assess whether a new VRRP configuration is required or whether an existing VRRP configuration can be modified or removed:

| | |
|---|---|
| Virtual Router ID | A numerical index (from 1 - 255) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router for which a packet is reporting status. |
| Description | A description assigned to the VRRP configuration when it was either created or modified. The description is implemented to provide additional differentiation beyond the numerical virtual router ID. |
| Virtual IP Addresses | The virtual interface IP address used as the redundant gateway address for the virtual route. |
| Interface | The interfaces selected on the access point to supply VRRP redundancy failover support. |
| Priority | A numerical value (from 1 - 254) used for the virtual router master election process. The higher the numerical value, the higher the priority in the election process. |

*Adding and Editing VRRP Configuration*

You can add a new VRRP configuration or edit an existing configuration to match changing network requirement.

1 Click **Add** to create a new VRRP configuration.

Click **Edit** to modify or override the attributes of a existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by clicking **Delete**.

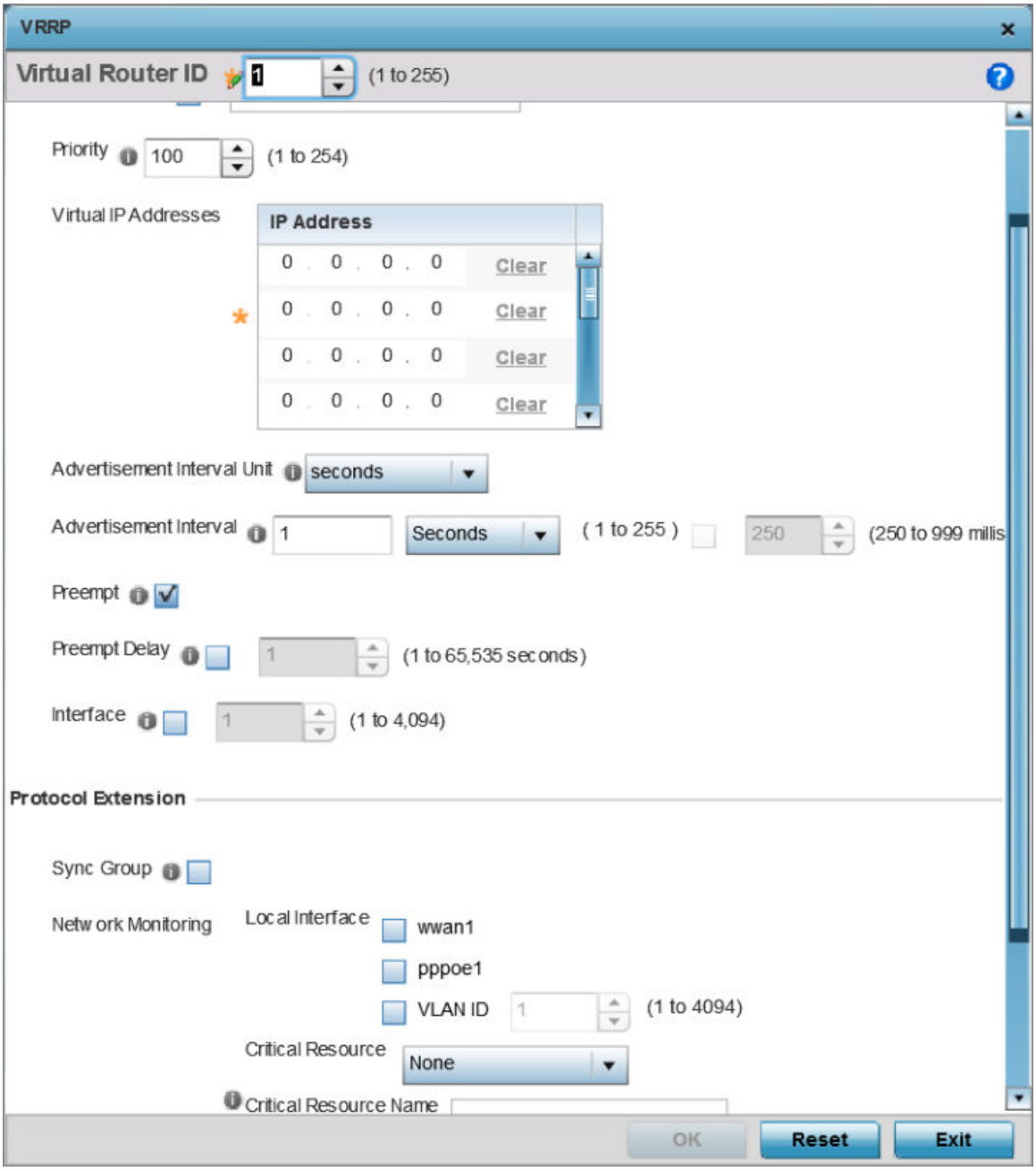



**Figure 104: Profiles - VRRP screen**

2 If you are creating a new VRRP configuration, assign a **Virtual Router ID** from 1 - 255.

In addition to functioning as numerical identifier, the ID identifies the virtual router for which a packet is reporting status.

3 Define the following VRRP General parameters:

| | |
|---|---|
| Description | In addition to an ID assignment, a virtual router configuration can be assigned a textual description (up to 64 characters) to further distinguish it from others with a similar configuration. |
| Priority | Use the spinner control to set a VRRP priority setting from 1 - 254. The controller or service platform uses the defined setting as criteria in selection of a virtual router master. The higher the value, the greater the likelihood of this virtual router ID being selected as the master. |
| Virtual IP Addresses | Provide up to eight IP addresses representing the Ethernet switches, routers, or security appliances defined as virtual router resources. |
| Advertisement Interval Unit | Select either **seconds**, **milliseconds** or **centiseconds** as the unit used to define VRRP advertisements. After an option is selected, the spinner control becomes enabled for that Advertisement Interval option. The default interval unit is seconds.<br>If you are changing the VRRP group version from 2 to 3, the advertisement interval must be in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds. |
| Advertisement Interval | After selecting an *Advertisement Interval Unit* , use the spinner control to set the interval the VRRP master sends out advertisements on each of its configured VLANs. The default setting is 1 second. |
| Preempt | Select this option to ensure a high priority backup router is available to preempt a lower priority backup router resource. The default setting is enabled. When selected, the *Preempt Delay* option becomes enabled to set the actual delay interval for pre-emption. This setting determines if a node with a higher priority can take over all the Virtual IPs from the nodes with a lower priority. |
| Preempt Delay | If the *Preempt* option is selected, use the spinner control to set the delay interval (in seconds) for preemption. |
| Interface | Select this value to enable or disable VRRP operation and define the VLAN (1 - 4,094) interface where VRRP will be running. These are the interfaces monitored to detect a link failure. |

4 Refer to the Protocol Extension field to define the following:

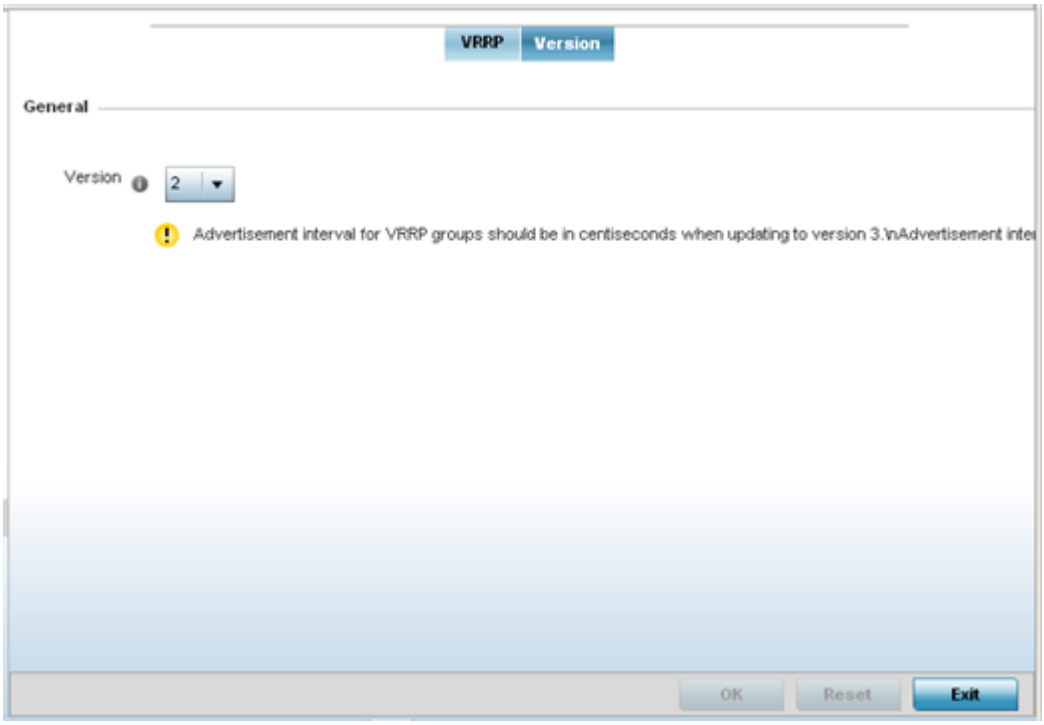
| | |
|---|---|
| Sync Group | Select the option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP fail over if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled by default. |
| Network Monitoring: Local Interface | Select wwan1, pppoe1, and VLAN ID(s) as needed to extend VRRP monitoring to these local access point interfaces. Once selected, these interfaces can be assigned an increasing or decreasing level or priority for virtual routing in the VRRP group. |
| Network Monitoring: Critical Resource | Assign the priority level for the selected local interfaces. Backup virtual routers can increase or decrease their priority in case the critical resources connected to the master router fail, and then transition to the master state themselves. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include **None**, **increment-priority** and **decrement priority**. |
| Network Monitoring: Delta Priority | Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring is enabled, the value is incremented by the setting defined. |

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

Click **Reset** to revert to the last saved configuration.

*Version*

1 Select the **Version** tab to define the VRRP version scheme used with the configuration.




2 Assess the VRRP version configuration.

VRRP version 3 (RFC 5798) and 2 (RFC 3768) are options for router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. For more information on VRRP protocol specifications (available publicly) refer to *http://www.ietf.org/rfc/rfc3768.txt* (version 2) and *http://www.ietf.org/rfc/rfc5798.txt* (version 3).

3 From within VRRP tab, select **Add** to create a new VRRP configuration or **Edit** to modify the attributes of an existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by selecting Delete.

## List of Critical Resources

Critical resources are device IP addresses or interface destinations on the network inter-operated as critical to the health of the network. The critical resource feature allows for the continuous monitoring of these addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, a AAA server, a WAN interface, or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly by the access point. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, no critical resource policy is enabled, and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they are discovered. For example, a critical resource on the same subnet as the access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to monitored on that VLAN.

Critical resources can be configured for access points and wireless controllers using their respective profiles.

To define critical resources:

1 Select **Configuration → Devices → System Profile → Critical Resources** from the web UI.

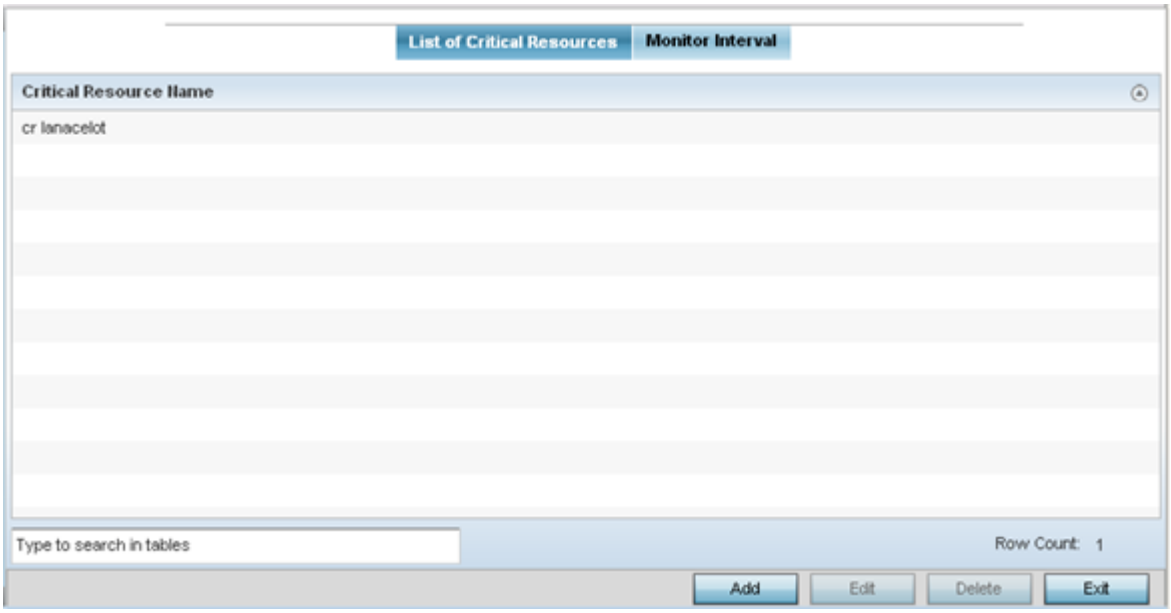



**Figure 105: Critical Resources Screen - List of Critical Resources tab**

2 Review the existing critical resources.

The screen lists the destination IP addresses or interfaces (VLAN, WWAN, or PPPoE) used for critical resource connection. IP addresses can be monitored directly by the access point or controller. However, a VLAN, WWAN, or PPPoE must be monitored behind an interface.

*Adding and Editing Critical Resources*

1 To set or override an existing critical resource configuration, click **Edit**.

Click **Add** to add a new critical resource and connection method.

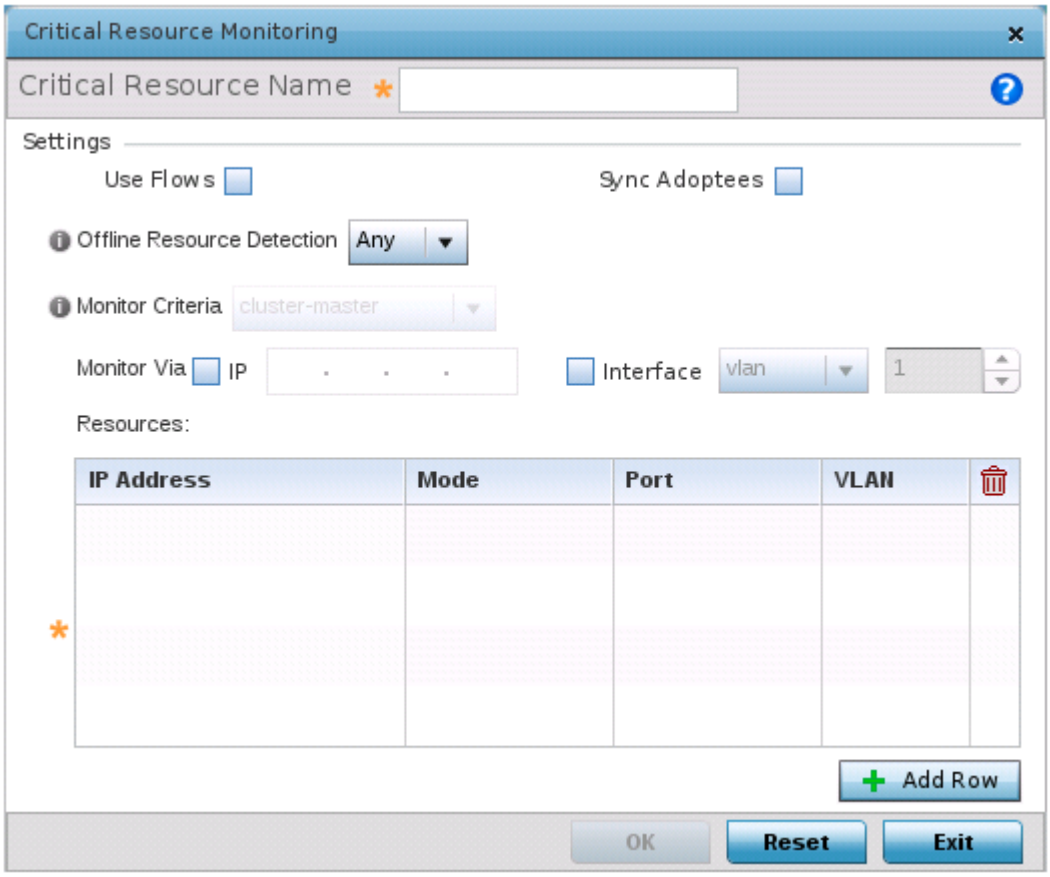



**Figure 106: Critical Resources Screen - Adding a Critical Resource**

2 If you are adding a new critical resource, in the Critical Resource Name field, provide a `name` up to 32 characters.

3 Select **Use Flows** so that the critical resource will monitor using firewall flows for DHCP or DNS instead of ICMP or ARP packets.

This reduces the amount of traffic on the network. This setting is disabled by default.

4 Select **Sync Adoptees** to sync adopted devices to state changes with a resource-state change message .

This setting is disabled by default.

5 Use the **Offline Resource Detection** drop-down menu to define how critical resource event messages are generated.

Options include **`Any`** and **`All`**. If you select **`Any`**, an event is generated when the state of any single critical resource changes. If you select **`All`**, an event is generated when the state of all monitored critical resources change.

6 Use the **Monitor Criteria** drop-down menu to select either **`rf-domain-manager`**, **`cluster-master`** or **`All`** as the resource for monitoring critical resources by one device and updating the rest of the devices in a group.

If you select rf-domain-manager, the current rf-domain manager performs resource monitoring, and the rest of the devices do not. The RF-domain-manager updates any state changes to the rest of the devices in the RF Domain.

With the cluster-master option, the cluster master performs resource monitoring and updates the cluster members with state changes.

With a controller-managed RF Domain, set **Monitoring Criteria** to **`All`** because the controller might not know the VLAN bridged locally by the devices in the RF Domain monitoring DHCP.

7 In the Monitor Via field, select the **`IP`** option to monitor a critical resource directly (within the same subnet) using the provided IP address as a network identifier.

8 In the Monitor Via field, select the **Interface** check box to monitor a critical resource using the critical resource's **`VLAN`**, **`WWAN1`** or **`PPPoE1`** interface.

If you select **`VLAN`**, use the spinner control to define the destination VLAN ID used as the interface for the critical resource.

9 In the Resources table, click **+ Add Row** and define the following parameters:

| | |
|---|---|
| IP Address | Provide the IP address of the critical resource. This is the address used by the access point to ensure the critical resource is available. Up to four addresses can be defined. |
| Mode | Set the ping mode used when the availability of a critical resource is validated. The options are:<br>• **`arp-only`** – Use only the ARP *(Address Resolution Protocol)* for pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known.<br>• **`arp-and-ping`** – Use both ARP and ICMP *(Internet Control Message Protocol)* for pinging the critical resource and sending control messages (for example, *device not reachable* or *requested service not available*). |
| Port | Provide the port on which the critical resource is available. Use the spinner control to set the port number. |
| VLAN | Using the spinner control, define the VLAN on which the critical resource is available. |

10 Click **OK** to save the critical resource configuration changes.

Click **Reset** to revert to the last saved configuration.

*Monitor Interval*

To override the critical resource monitoring interval configuration:

1 Select the **Monitor Interval** tab.

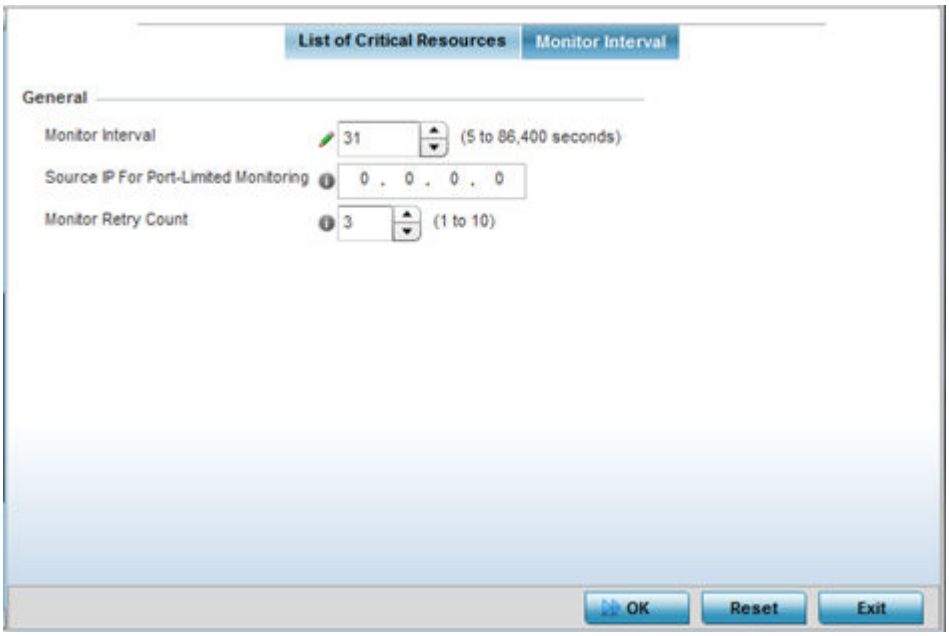



**Figure 107: Critical Resources Screen - Monitor Interval Tab**

2 Use **Monitor Interval** screen to set the duration, in seconds, between two successive pings to the critical resource.

Select a duration between 5 and 86,400 seconds. The default setting is 30 seconds.

3 Use **Source IP for Port-Limited Monitoring** to define the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface.

Generally, the source address 0.0.0.0 is used in the ARP packets used to detect critical resources. However, some devices do not support that IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for Port-Limited Monitoring must be different from the IP address configured on the device.

4 Use **Monitor Retry Count** to set the number of retry connection attempts (1 - 10) permitted before this device connection is defined as down (offline).

The default setting is three connection attempts.

5 Click **OK** to save the and monitor interval changes.

Click **Reset** to revert to the last saved configuration.

## Profile Services Configuration

A profile can contain specific guest access (captive portal) server configurations. These guest network access permissions can be defined uniquely as profile requirements dictate.

Before defining a profile's captive portal and DHCP configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- A profile plan should consider the number of wireless clients allowed on the profile's guest (captive portal) network and the services provided, or if the profile should support guest access at all.

- Profile configurations supporting a captive portal should include firewall policies to ensure logical separation is provided between guest and internal networks so internal networks and hosts are not reachable from guest devices.
- DHCP's lack of an authentication mechanism means a DHCP server supported profile cannot check if a client or user is authorized to use a given user class. This introduces a vulnerability when using user class options. Ensure a profile using DHCP resources is also provisioned with a strong user authorization and validation configuration.

To define a profile's services configuration:

1 Select **Configuration → Devices → System Profile → Services**.

2 Refer to the Profile_Captive_Portal field to select or set a guest access configuration (captive portal) for use with this profile.

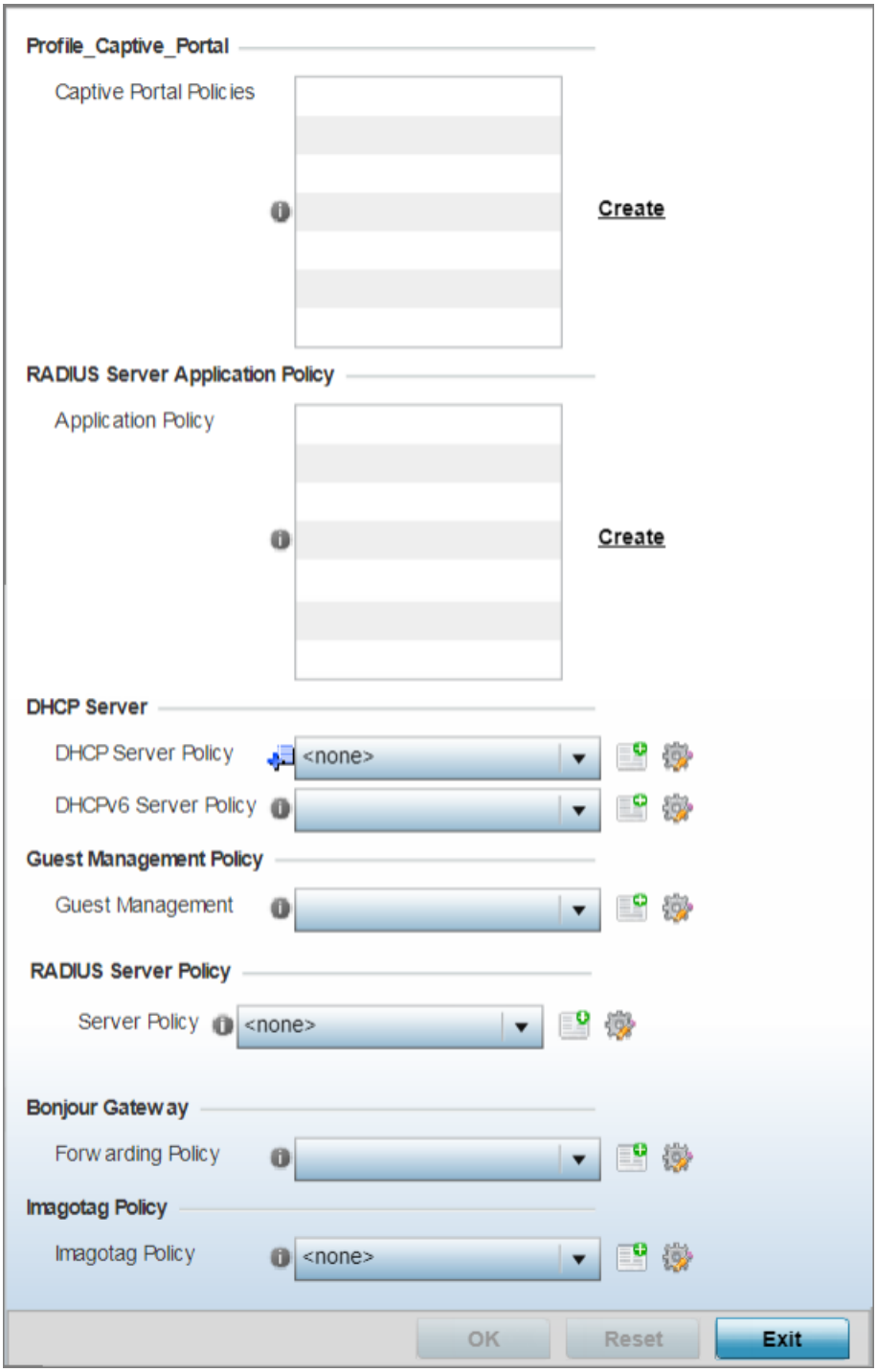



**Figure 108: Profile Services - Services Screen**

A captive portal is guest access policy for providing guests temporary and restrictive access to the access point managed network.

A captive portal provides secure authenticated access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Agreement, Welcome and Fail pages provide the administrator with a number of options on screen flow and user appearance.

3 Select an existing captive portal policy, use the default captive portal policy or select the **Create** link to create a new captive portal configuration that can be applied to this profile.

For more information, see Captive Portal Policies on page 785.

4 Use the **RADIUS Server Application Policy** drop-down menu to select an application policy to authenticate users and authorize access to the network.

A RADIUS policy provides the centralized management of authentication data (usernames and passwords). When an client attempts to associate, the controller or service platform sends the authentication request to the RADIUS server. If an existing RADIUS server policy does not meet your requirements, click the Create link to create a new policy.

5 Use the **DHCP Server Policy** drop-down menu assign this profile a DHCP server policy. If an existing DHCP policy does not meet the profile's requirements, click the Create icon to create a new policy configuration that can be applied to this profile, or click the Edit icon to modify the parameters of an existing DHCP Server policy.

*Dynamic Host Configuration Protocol* (DHCP) allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the onboard DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an predetermined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. When the lease expires, the client is no longer permitted to use the leased IP address. The profile's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired).

6 Use the **DHCPv6 Server Policy** drop-down menu assign this profile a DHCPv6 server policy. If an existing DHCP policy for IPv6 does not meet the profile's requirements, click the Create icon to create a new policy configuration that can be applied to this profile, or click the Edit icon to modify the parameters of an existing DHCP Server policy.

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network. DHCP in IPv6 works in with IPv6 router discovery. With the proper RA flags, DHCPv6 works like DHCP for IPv4. The central difference is the way a device identifies itself if assigning addresses manually instead of selecting addresses dynamically from a pool.

7 Use the **RADIUS Server Policy** drop-down menu to select an existing RADIUS server policy to use as a user validation security mechanism with this profile.

A profile can have its own unique RADIUS server policy to authenticate users and authorize access to the network. A profile's RADIUS policy provides the centralized management of controller or service platform authentication data (usernames and passwords). When an client attempts to associate, an authentication request is sent to the RADIUS server.

8 Refer to the **Bonjour Gateway** field to select or set a Bonjour Gateway Forwarding Policy.

Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour Forwarding Policy enables discovery of services on VLANs which are not visible to the device running the Bonjour Gateway. Bonjour forwarding enables forwarding of Bonjour advertisements across VLANs to enable the Bonjour Gateway device to build a list of services and the VLANs where these services are available.

9 Refer to the **Imagotag Policy** field to select or set a Imagotag Policy. Use the drop-down menu to select and apply an Imagotag Policy to the AP's profile. You can use the **Create** to create a new policy or **Edit** icon to edit an exisiting policy. The Imagotag feature is supported only on the AP-8432 model access point.

For more information on enabling support for SES-imagotag's ESL tags on AP-8432 APs with USB interfaces, see Setting the Imagotag Policy on page 845.

10 Select **OK** to save the changes made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

## Management Settings

There are mechanisms to allow or deny management access to the network for separate interfaces and protocols: HTTP, HTTPS, Telnet, SSH, and SNMP.

These management access configurations can be applied strategically to profiles as resource permissions dictate for the profile. Additionally, overrides can be applied to customize a device's management configuration, if deployment requirements change and a device's configuration must be modified from its original device profile configuration.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support. You can override the management configurations of a profile at the device level. To override an access point profile's management settings:

To define or override a profile's management configuration:

1 Go to **Configuration → Devices → System Profile**.

2 Select an access point.

The selected access point's profile configuration menu displays.

3 Expand **Profile Overrides** → **Management**.

Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

The management Settings configuration screen displays.

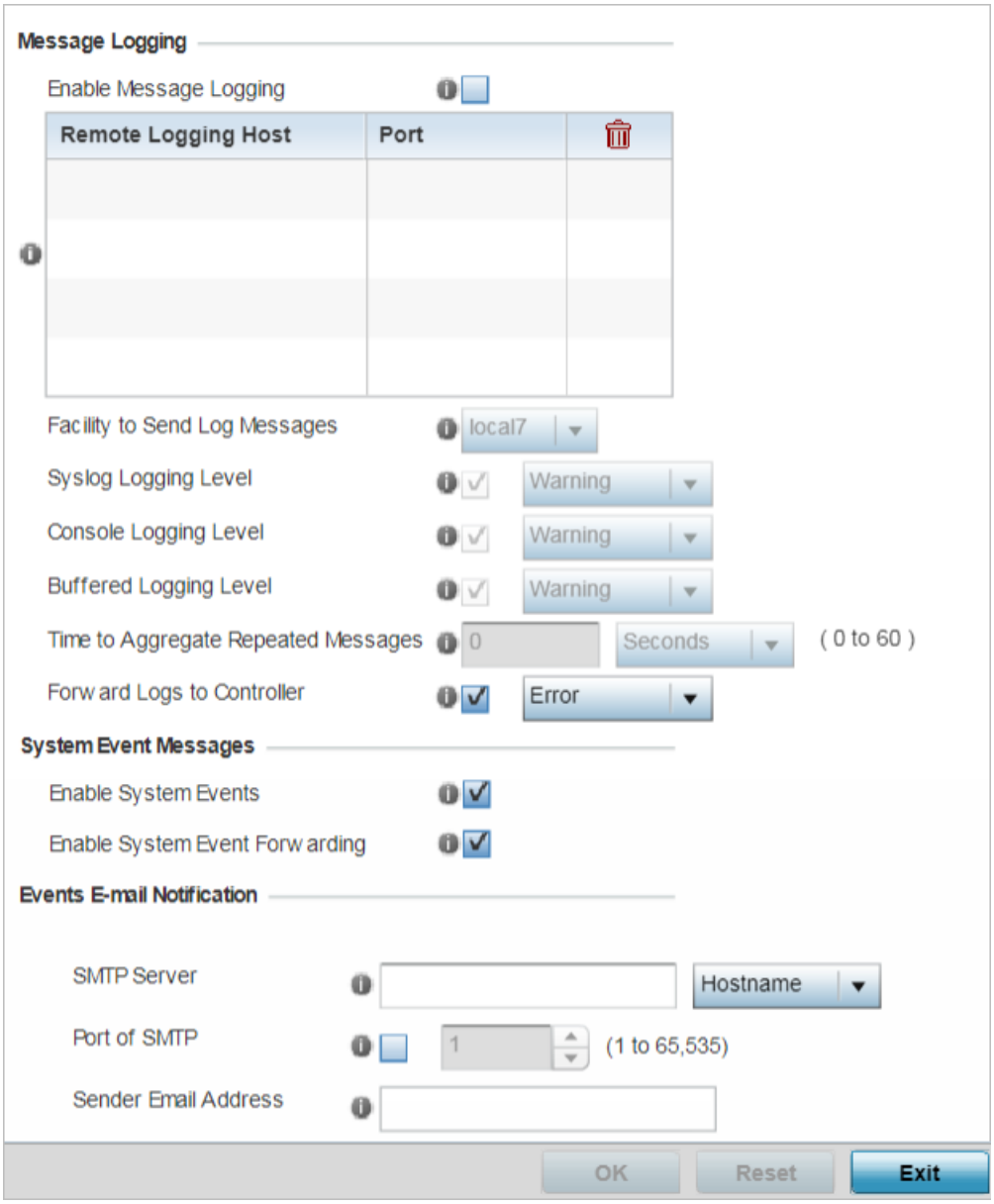



**Figure 109: Profile Overrides - Management - Settings Configuration Screen**

4 In the Message Logging field, select the **Enable Message Logging** checkbox to enable message logging. When enabled, system events are logged to a log file or a syslog server.

Selecting this check box enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.

5 In the Remote Logging Host table provide the following:

| | |
|---|---|
| Remote Logging Host | Define numerical (non DNS) IP addresses for up to four external resources where logged system events can be sent by the access point. Select the trash icon as needed to remove an IP address from the list. |
| Port | Define the ports at which the external resources are reachable. |

6 Configure the following Message Logging parameters:

| | |
|---|---|
| Facility to Send Log Messages | Use the drop-down menu to specify the local server (if used) for access point event log transfers. |
| System Logging Level | Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include: **0 - Emergency**, **1 - Alert**, **2 - Critical**, **3 - Errors**, **4 - Warning**, **5 - Notice**, **6 - Info** and **7 - Debug**. The default logging level is *4 - Warning*. |
| Console Logging Level | Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include: **0 - Emergency**, **1 - Alert**, **2 - Critical**, **3 - Errors**, **4 - Warning**, **5 - Notice**, **6 - Info** and **7 - Debug**. The default logging level is *4 - Warning*. |
| Buffered Logging Level | Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include: **0 - Emergency**, **1 - Alert**, **2 - Critical**, **3 - Errors**, **4 - Warning**, **5 - Notice**, **6 - Info** and **7 - Debug**. The default logging level is *4 - Warning*. |
| Time to Aggregate Repeated Messages | Define the increment (or interval) system events are logged on behalf of the access point. The shorter the interval, the sooner the event is logged. Either define an interval in seconds (0 - 60) or minutes (0 -1). The default value is 0 seconds. |
| Forward Logs to Controller | Select this option to define a log level for forwarding event logs to the control. Log levels include Emergency, Alert, Critical, Error, Warning, Notice, Info and Debug. The default logging level is Error. |

7 Refer to the System Event Messages field to define or override how system messages are logged and forwarded on behalf of the profile.

a Select **Enable System Events** to allow the profile to capture system events and append them to a log file.

It is important to log individual events to discern an overall pattern that may be negatively impacting performance. This setting is enabled by default.

b Select **Enable System Event Forwarding** to enable the forwarding of system events.

This setting is enabled by default.

8 Refer to the Events E-mail Notification field to define or override how system event notification emails are sent.

| | |
|---|---|
| SMTP Server | Specify either the hostname or IP address of the outgoing SMTP server where notification emails are originated. |
| Port of SMTP | If a non-standard SMTP port is used on the outgoing SMTP server, select this option and specify a port from 1 - 65,535 for the outgoing SMTP server to use. |
| Sender E-mail Address | Specify the email address from which notification email is originated. This is the *from* address on notification email. |

| | |
|---|---|
| Recipient's E-mail Address | Specify one or more email addresses to be the recipients of event email notifications. |
| Username for SMTP Server | Specify the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with an username and password before sending email through the server. |
| Password for SMTP Server | Specify password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with an username and password before sending email through the server. |

9 In the Persist Configuration Across Reloads field, use the **Configure** drop-down menu to define whether the access point saves a configuration received from a Virtual Controller AP to flash memory.

The configuration would then be made available if the this access point reboots and the Virtual Controller AP is not reachable. Options include **`Enabled`**, **`Disabled`**, and **`Secure`**.

10 Refer to the HTTP Analytics field to define analytic compression settings and update intervals.

| | |
|---|---|
| Compress | Select this option to use data compression to when sending updates to the controller. |
| Update Interval | Set the interval – in minutes, seconds, or hours – when the collected data is sent to the external analytics engine. |

11 Click **OK** to save the management setting overrides.

Click **Reset** to revert to the last saved configuration.

*Management Firmware*

To configure the access point profile's firmware upgrade settings:

1 Select **Management → Firmware**.

The management Firmware upgrade setting configuration screen displays.

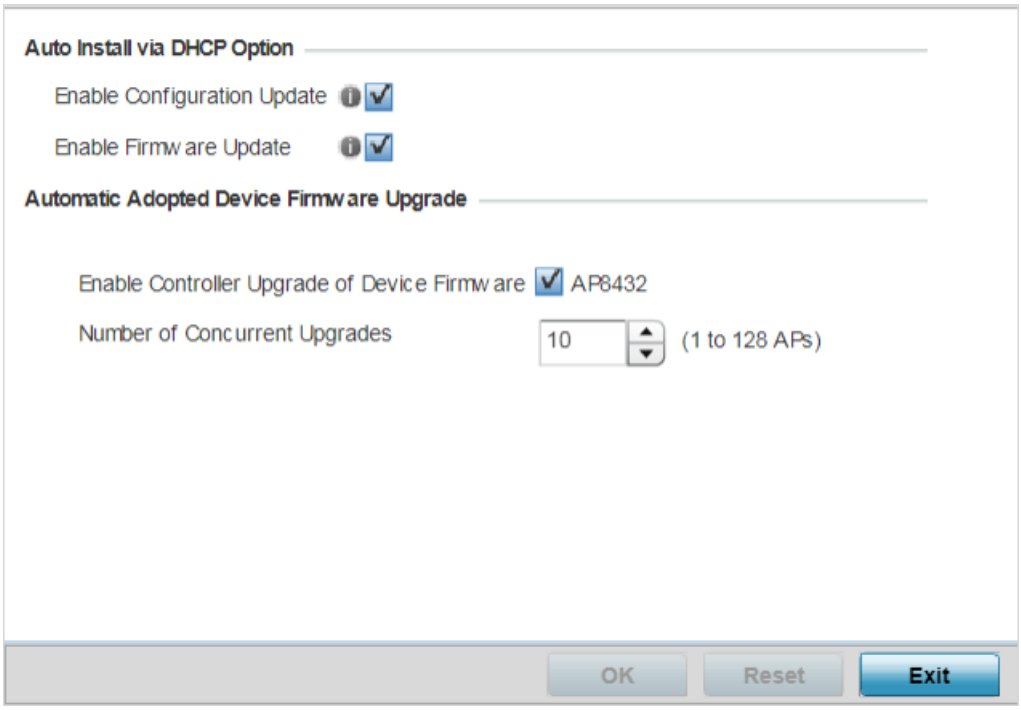



**Figure 110: Management - Firmware Upgrade Configuration Screen**

2 Refer to the Auto Install via DHCP Option field to configure automatic configuration file and firmware updates.

| | |
|---|---|
| Enable Configuration Update | Select this option to enable automatic configuration file updates for the controller profile from a location external to the access point. |
| Enable Firmware Update | Select this option to enable automatic firmware updates for this profile from a user-defined remote location. This value is disabled by default. |

3 In the Automatic Adopted Device Firmware Upgrade section, define an automatic firmware upgrade from a local file.

| | |
|---|---|
| Enable Controller Update of Device Firmware | Select the access point model to upgrade using its associated Virtual Controller AP's most recent firmware file for that model. This parameter is enabled by default. |
| Number of Concurrent Upgrades | Use the spinner control to define the maximum number (1 - 128) of adopted APs that can receive a firmware upgrade at the same time. Keep in mind that during a firmware upgrade, the access point is offline and unable to perform its normal client support role until the upgrade process is complete.<br><br>Note:<br>This is applicable in case the access point is a virtual controller. |

4 Click **OK** to save the management firmware overrides.

Click **Reset** to revert to the last saved configuration.

*Management Heartbeat*

To configure the access point profile's management heartbeat configuration:

1 Select **Management → Heartbeat**.

The management Heartbeat setting configuration screen displays.

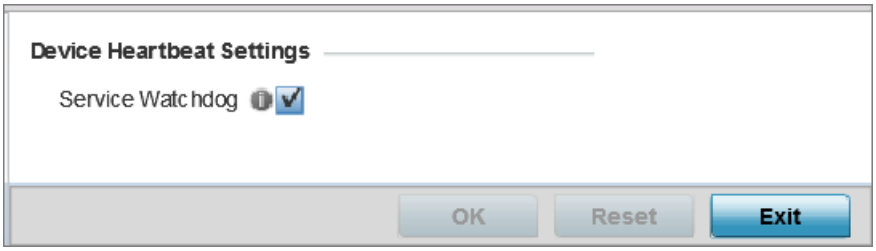



**Figure 111: Management - Heartbeat Configuration Screen**

2 Select the **Service Watchdog** option to implement heartbeat messages.

This ensures that associated devices are up and running and can interoperate effectively. The Service Watchdog is enabled by default.

3 Click **OK** to save the changes and overrides made to the profile's configuration.

Click **Reset** to revert to the last saved configuration.

## Meshpoint Configuration

An access point can be configured to be a part of a meshed network. A mesh network is one where nodes in the network can communicate with each where each node can maintain more than one path to its peers. Mesh networking enables users to access broadband applications anywhere, including moving vehicles, by providing robust, reliable, and redundant connectivity to all the members of the network. When one of the nodes in a mesh network becomes unavailable, the other nodes in the network can still communicate with each other directly or through intermediate nodes.

*Mesh point* is the name given to a device that is a part of a meshed network.

Use the Mesh Point screen to configure or override the parameters that set how this device behaves as a part of the mesh network.

Note

WiNG 7.1 release does not support MeshConnex on AP505i and AP510i model access points. This feature will be supported in future releases.

To set or override a profile's mesh point configuration:

1 Select **Configuration → Devices → System Profiles** from the web UI.

A list of profiles is displayed in the right-hand UI.

2 Select **Mesh Point** from the menu.

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

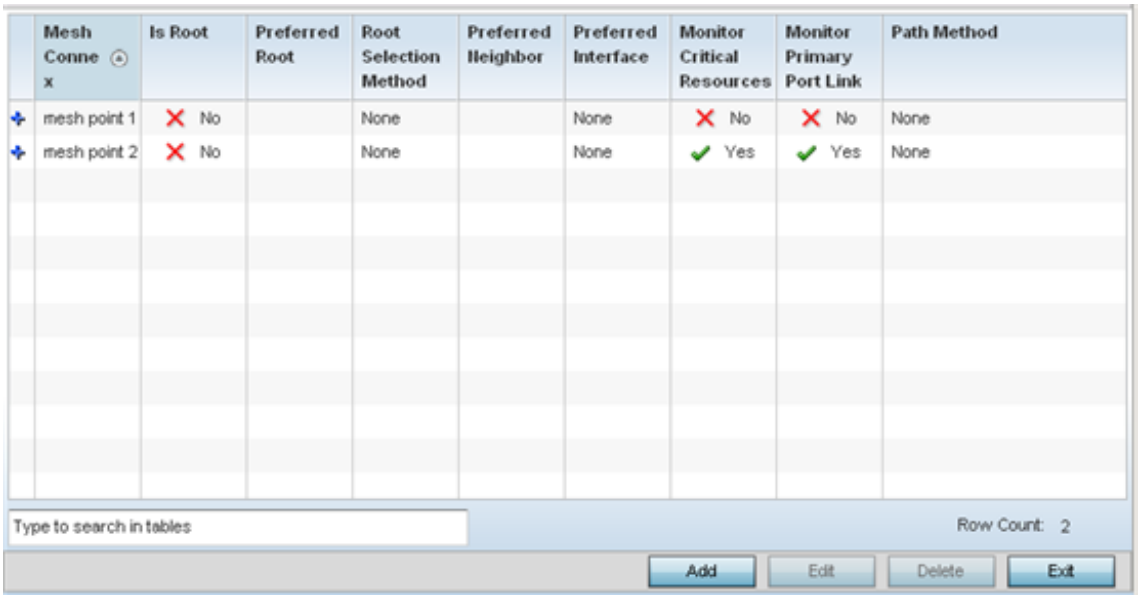



**Figure 112: Device Overrides - Mesh Point Screen**

3 Review existing meshpoints to determine if a new meshpoint warrants creation or an existing meshpoint needs to be edited.

*Adding and Editing Meshpoint Settings*

You can add a new meshpoint configuration or edit an existing meshpoint configuration.

1 Click **Add** to create a new mesh point configuration, if an existing configuration does not meet your requirements.

Click **Edit** to modify or override the attributes of a existing mesh point configuration. If necessary, existing configurations can be selected and permanently removed by clicking **Delete**.

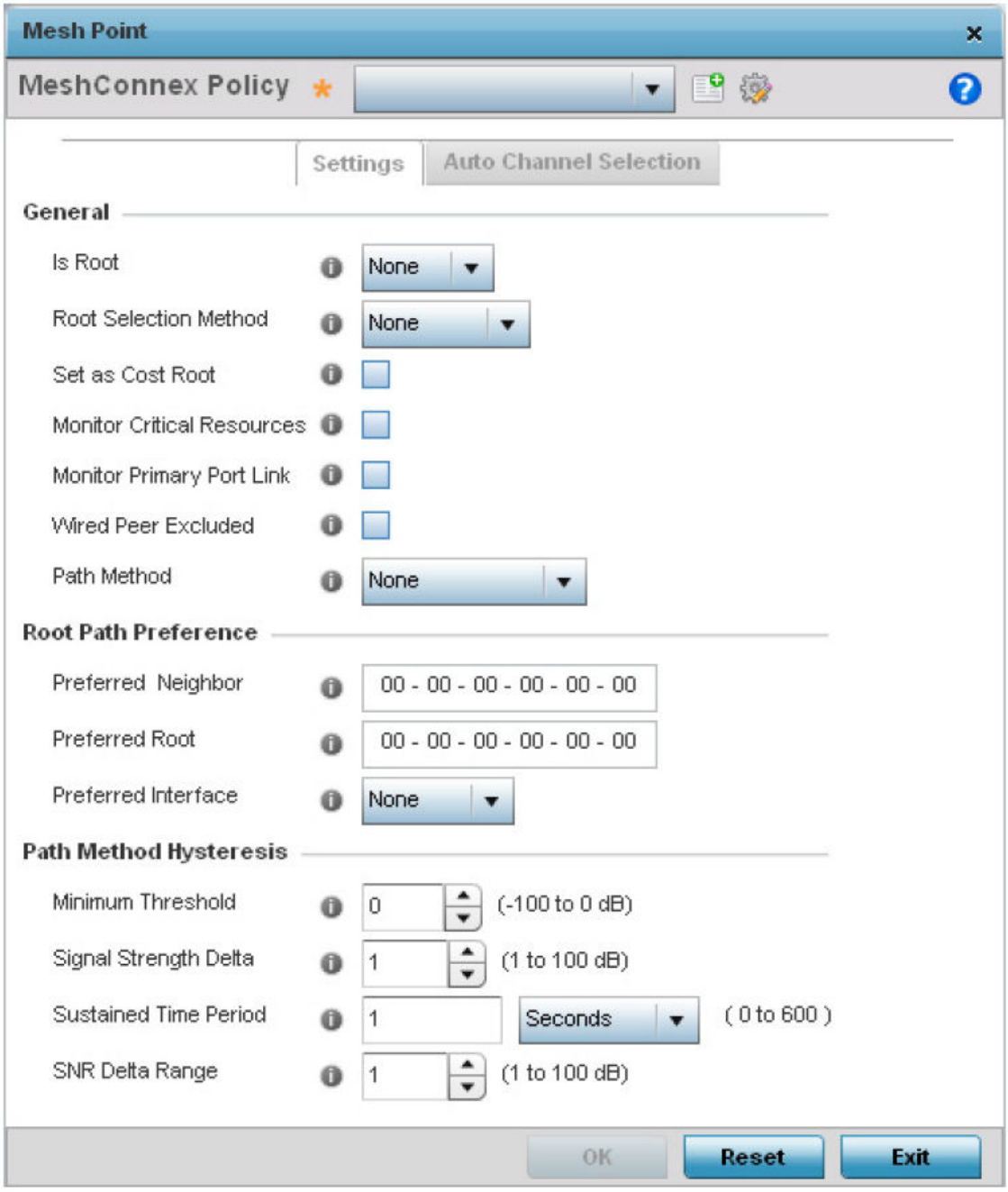



**Figure 113: Mesh Point Settings Screen**

2 Define the following General mesh point settings:

| | |
|---|---|
| MeshConnex Policy | Provide a name for the Mesh Connex Policy. Use the **Create** icon to create a new Mesh Connex Policy. To edit an existing policy, select it from the dropdown and click the **Edit** icon. For more information on creating or editing a Mesh Connex Policy, see MeshConnex Policies on page 646. |
| Is Root | Select the root behavior of this access point. **`True`** means that this access point is a root node for this mesh network, and **`False`** means that it is not a root node. A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. |
| Root Selection Method | Use the drop-down menu to determine whether this mesh point is the root or non-root mesh point. Select either **`None`** (the default setting) or **`auto-mint`**. |
| Set as Cost Root | Select this option to set the mesh point as the cost root for mesh point root selection. This setting is disabled by default. |
| Monitor Critical Resources | Select this option to enable critical resource monitoring for this mesh point. |
| Monitor Primary Port Link | Select to enable monitoring of primary port link is enabled for this mesh connex policy. If the primary port link is not present and if the device is a mesh root, it is automatically changed to a non-root device. When the primary port link becomes available again, the non-root device is changed back to a root device. |
| Wired Peer Exclude | Select this option to exclude wired peers when creating mesh links. |
| Path Method | Select the method used for path selection in a mesh network. Available options include:<br>• **`None`** – No criteria are used in root path selection.<br>• **`uniform`** – The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths).<br>• **`mobile-snr-leaf`** – The access point is mounted on a vehicle or a mobile platform (WiNG models only). The path to the route is selected based on the SNR *(Signal To Noise Ratio)* with the neighbor device.<br>• **`snr-leaf`** – The path with the best signal to noise ratio is always selected. |
| Minimum Threshold | Enter the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered. This field along with Signal Strength Delta and Sustained Time Period are used to dynamically select the next hop in a dynamic mesh network.The default setting is 0 dB. |
| Signal Strength Delta | Enter a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR higher than the value configured here. This field along with the Minimum Threshold and Sustained Time Period are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 dB. |

| | |
|---|---|
| Sustained Time Period | Enter the time duration in seconds (0 - 600) or minutes (0 - 10). This indicates the duration that a signal must sustain the constraints specified in the Minimum Threshold and Signal Strength Delta path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 second. |
| SNR Delta Range | Select the root selection method hysteresis (from 1 - 100dB) SNR delta range a candidate must sustain. The default setting is 1 dB. |

**Note**

An AP 7161 model access point can be deployed as a VMM *(vehicular mounted modem)* to provide wireless network access to a mobile vehicle such as a car or train. A VMM provides layer 2 mobility for connected devices. VMM does not provide layer 3 services, such as IP mobility. For VMM deployment considerations, see Vehicle Mounted Modem (VMM) Deployment Considerations on page 278.

3 Set the following **Root Path Preference** values:

| | |
|---|---|
| Preferred Neighbor | Specify the MAC address of a preferred neighbor for this mesh point. |
| Preferred Root | Specify the MAC address of a preferred mesh root for this mesh point. |
| Preferred Interface | Select the preferred Interface for this mesh point. Select **None** to set no preferences. The other interface choices are 2.4 GHz and 5 GHz. |

*Adding and Editing ACS Dynamic Root Selection Configuration*

1 Click the **Auto Channel Selection** tab to configure the parameters for the MeshConnex Auto Channel Selection policy.

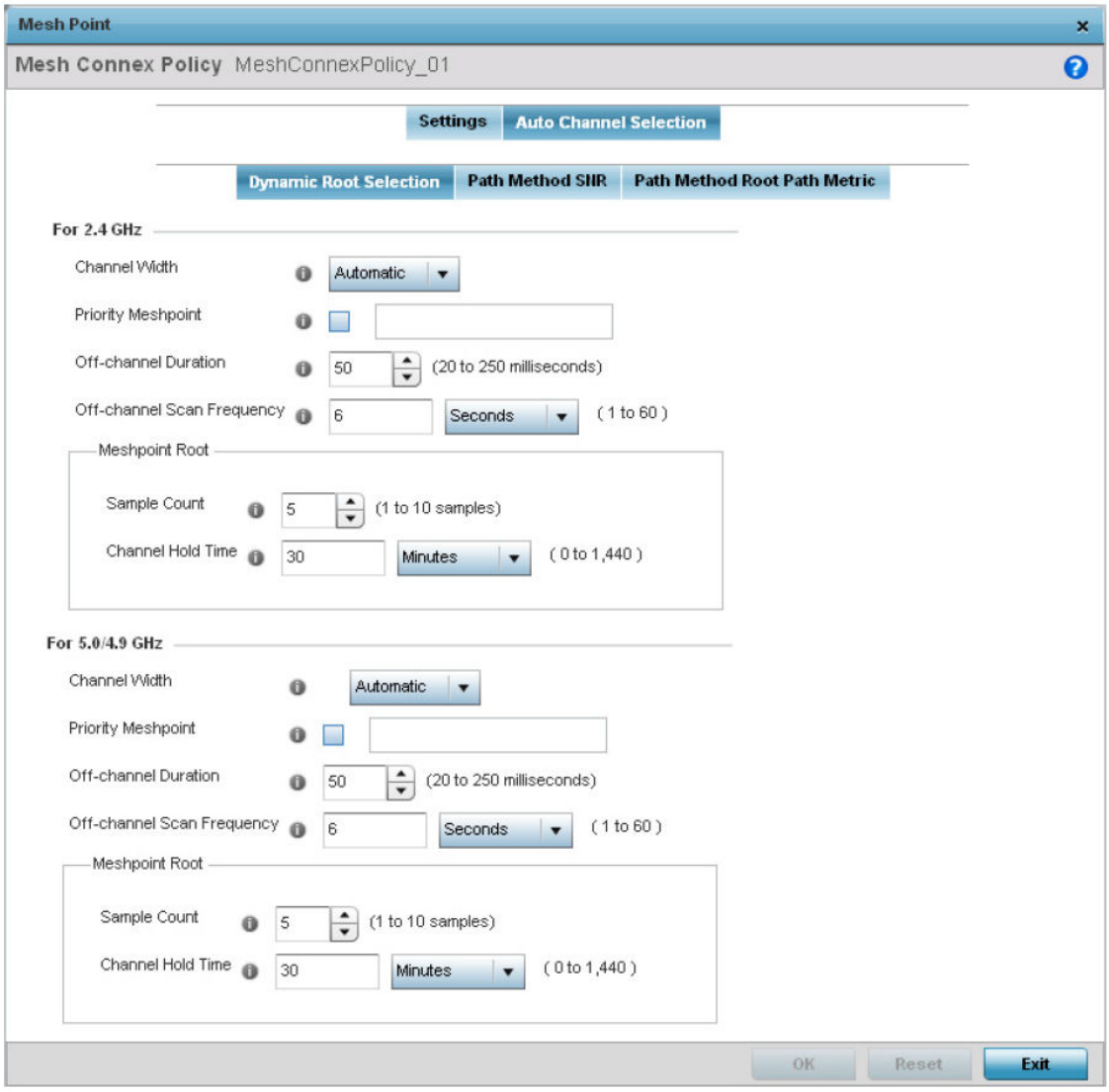



**Figure 114: Mesh Point Auto Channel Selection Screen - Dynamic Root Selection Tab**

The Dynamic Root Selection screen displays by default. This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies.

2 Refer to the following for more information on the **Auto Channel Selection → Dynamic Root Selection** screen. These descriptions are common for configuring the 2.4 GHZ and 5.0/4.9 GHz frequencies.

| | |
|---|---|
| Channel Width | Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include:<br>• **`Automatic`** – The channel width is calculated automatically. This is the default value.<br>• **`20 MHz`** – Sets the width between adjacent channels as 20 MHz.<br>• **`40 MHz`** – Sets the width between adjacent channels as 40 MHz. |
| Priority Meshpoint | Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. |
| Off-channel Duration | Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds. |
| Off-channel Scan Frequency | Set the duration (from 1- 60 seconds) between two consecutive off channel scans. The default is 6 seconds. |
| Meshpoint Root: Sample Count | Configure the number of scan samples (from 1- 10) for data collection before a mesh channel is selected. The default is 5. |
| Meshpoint Root: Channel Hold Time | Configure the duration (from 0 - 1440 minutes) to remain on a channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring.The default setting is 30 minutes. |

3 Click **OK** to save the changes made to the mesh point configuration.

Click **Reset** to revert to the last saved configuration.

### Adding and Editing ACS Path Method SNR Configuration

1 Select the **Path Method SNR** tab to configure SNR ratio values when selecting the path to the meshpoint root.

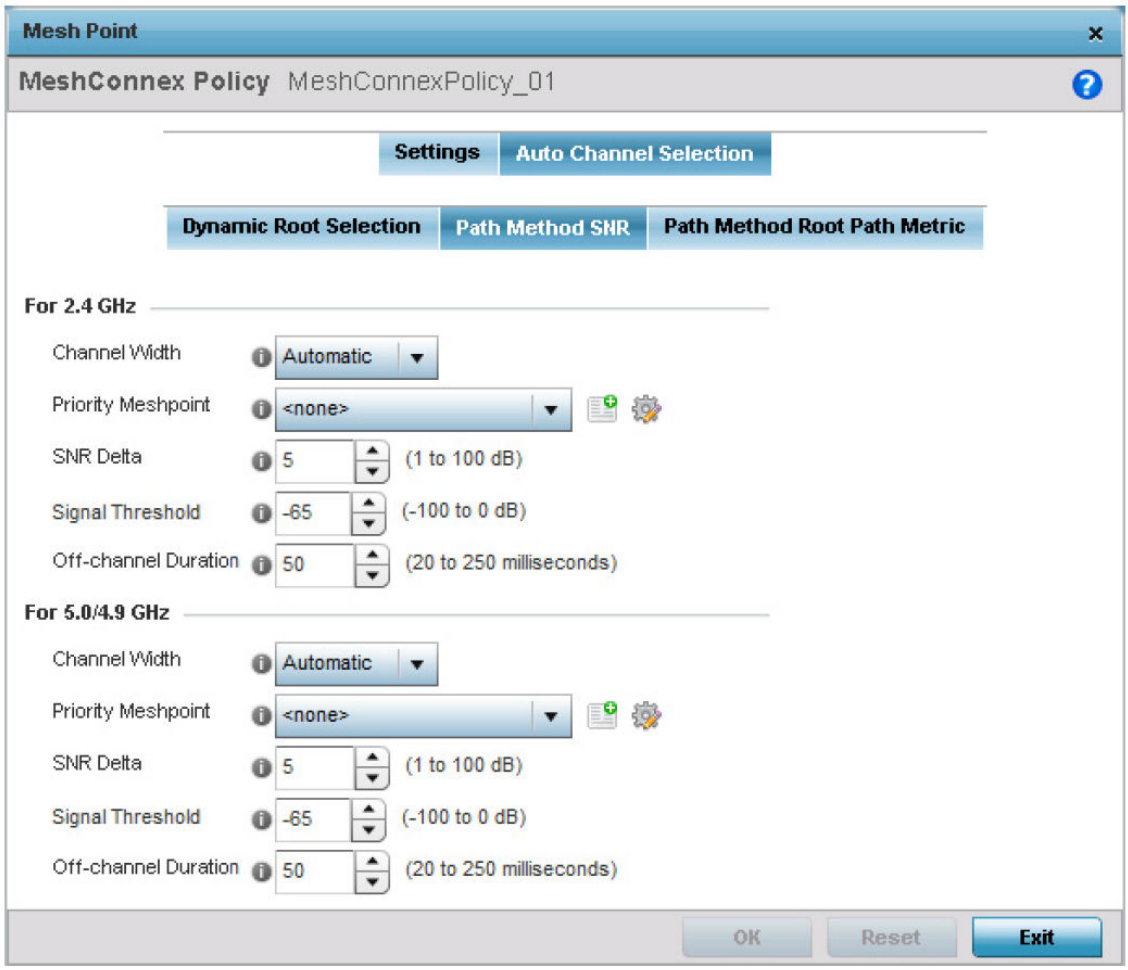



**Figure 115: Mesh Point Auto Channel Selection Screen - Path Method SNR Tab**

2 Set the following configuration for both **2.4 GHz** and **5.0/4.9 GHz**:

| | |
|---|---|
| Channel Width | Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include:<br>• **`Automatic`** – The channel width is calculated automatically. This is the default value.<br>• **`20 MHz`** – Sets the width between adjacent channels as 20 MHz.<br>• **`40 MHz`** – Sets the width between adjacent channels as 40 MHz. |
| Priority Meshpoint | Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. |
| SNR Delta | Set the SNR ratio delta (from 1 - 100 dB) for mesh path selections.<br>When path selection occurs, the defined value is utilized for selecting the optimal path. A better candidate, on a different channel, must have a signal strength that exceeds this delta value when compared to the signal strength of the next hop in the mesh network. The default setting is 5 dB. |

| | |
|---|---|
| SNR Threshold | Set the SNR threshold for mesh path selections (from -100 to 0 dB).<br>If the signal strength of the next mesh hop falls below this set value, a scan is triggered to select a better next hop. the default setting is -65 dB. |
| Off-channel Duration | Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds. |

3 Click **OK** to save the changes made to the mesh point configuration.
Click **Reset** to revert to the last saved configuration.

### Adding and Editing ACS Path Method Root Path Metric Configuration

1 Select the **Path Method Root Path Metric** tab to calculate root path metrics.

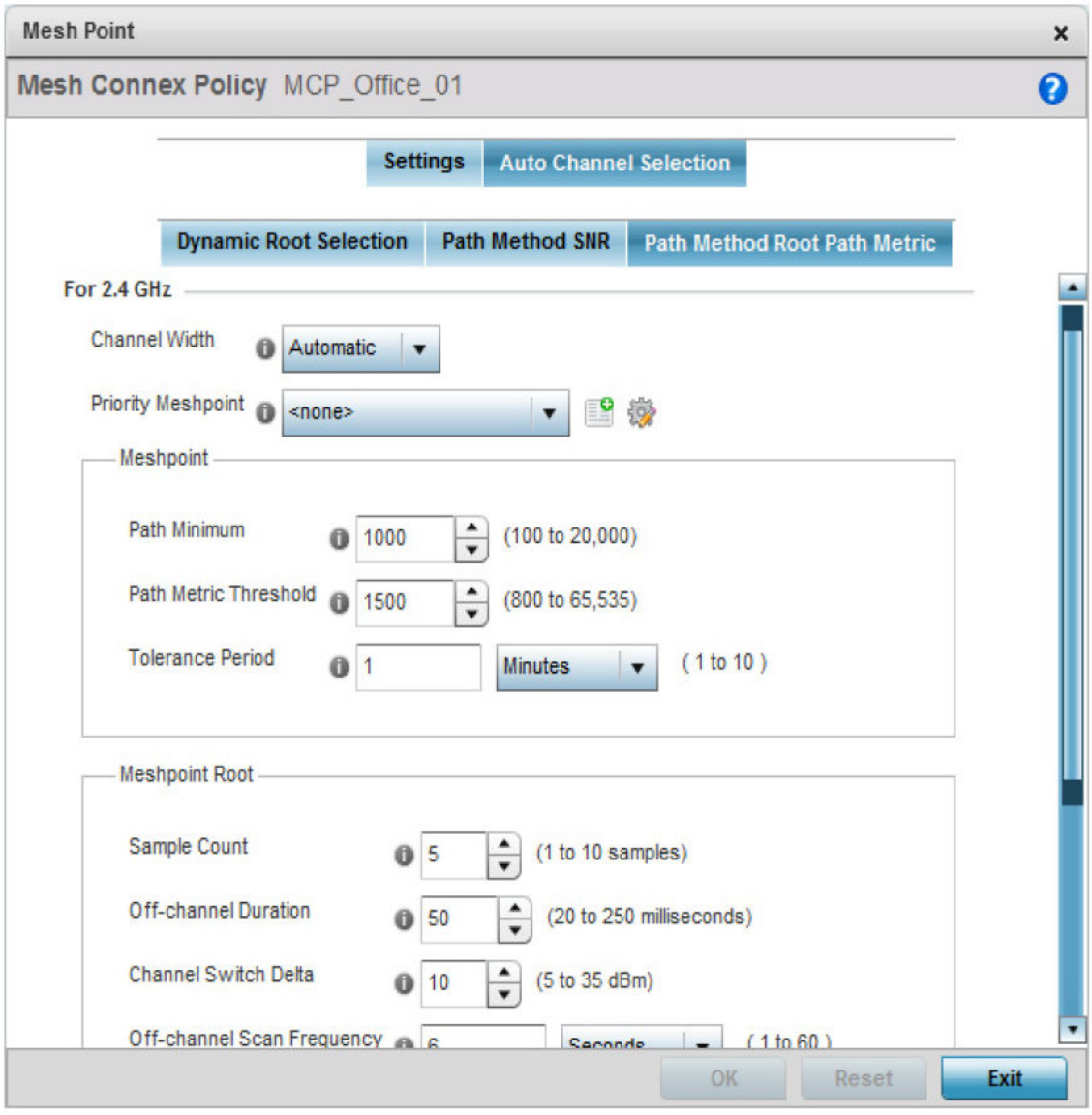



**Figure 116: Mesh Point Auto Channel Selection Screen - Path Method Root Path Metric Tab**

2 Set the following Path Method Root Path Metric values.
These descriptions apply to both the **2.4 GHz** and **5.0/4.9 GHz** frequencies.

| | |
|---|---|
| Channel Width | Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include:<br>• **`Automatic`** – The channel width is calculated automatically. This is the default value.<br>• **`20 MHz`** – Sets the width between adjacent channels as 20 MHz.<br>• **`40 MHz`** – Sets the width between adjacent channels as 40 MHz. |
| Priority Meshpoint | Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. |
| Meshpoint: Path Minimum | Set the minimum path metric (from 100 - 20,000) for establishing mesh connections. The default setting is 1000. |
| Meshpoint: Path Metric Threshold | Configure a minimum threshold (from 800 - 65535) for triggering an automatic channel selection for meshpoint selection. The default is 1500. |
| Meshpoint: Tolerance Period | Configure the duration to wait before triggering an automatic channel selection for the next hop. The default is 1 minute. |
| Meshpoint Root: Sample Count | Set the number of scans (from 1- 10) for data collection before a mesh point root is selected. The default is 5. |
| Meshpoint Root: Off-channel Duration | Configure the duration (from 20 - 250 milliseconds) that the scan dwells on each channel when performing an off-channel scan. The default is 50 milliseconds. |
| Meshpoint Root: Channel Switch Delta | Configure the delta (from 5 - 35 dBm) that triggers a meshpoint root automatic channel selection when exceeded. The default is 10 dBm. |
| Meshpoint Root: Off-channel Scan Frequency | Configure the duration (from 1 -60 seconds) between two consecutive off channel scans for meshpoint root. The default is 6 seconds. |
| Meshpoint Root: Channel Hold Time | Set the minimum duration (from 0 - 1440 minutes) to remain on a selected channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default is 30 minutes. |

3 Click **OK** to save the changes made to the mesh point configuration.

Click **Reset** to revert to the last saved configuration.

### *Vehicle Mounted Modem (VMM) Deployment Considerations*

Before defining a VMM configuration (mounting an AP7161 mesh point on a moving vehicle), refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Disable layer 2 stateful packet inspection from the firewall policy.
- Set the RTS threshold value to 1 on all mesh devices. The default value is 65,536. For more information on defining radio settings, see Access Point Radio Configuration on page 114.
- Use **`Opportunistic`** as the rate selection settings for the AP 7161 radio The default is **`Standard`**. For more information on defining this setting, see Profile Overrides - Radios on page 362.
- Disable Dynamic Chain Selection (radio setting). The default value is enabled. This setting is disabled from the Command Line Interface (CLI) using the `dynamic-chainselection` command, or, in the UI (refer to Profile Overrides - Radios on page 362).
- Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph. For more information, see Profile Overrides - Radios on page 362.

## Environmental Sensor Configuration

An AP 8132 sensor module is a USB environmental sensor extension to an AP 8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the AP 8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

To set or override an AP 8132 profile's environmental sensor configuration:

1 Select **Configuration → Devices → System Profile → Environmental Sensor**

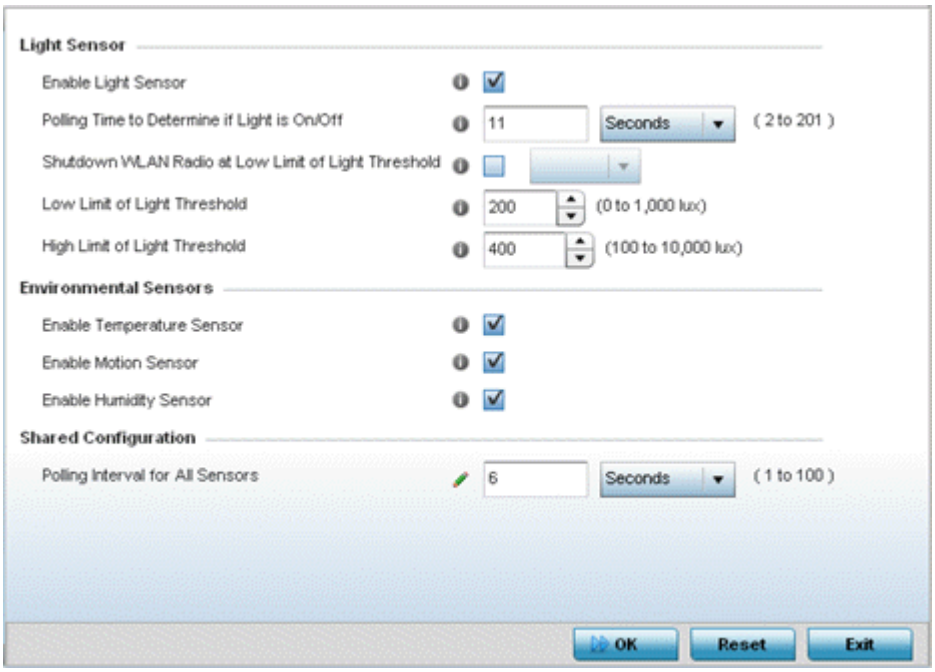



**Figure 117: Profile - Environmental Sensor Screen**

2 Set the following Light Sensor settings for the AP 8132's sensor module:

| | |
|---|---|
| Enable Light Sensor | Select this option to enable the light sensor on the module. This setting is enabled by default. The light sensor reports whether the AP 8132's deployment location has its lights powered on or off. |
| Polling Time to Determine if Light is On/Off | Define an interval in*Seconds* (2 - 201) or *Minutes* (1 - 4) for the sensor module to poll its environment to assess light intensity to determine whether lighting is on or off. The default polling interval is 11 seconds. Light intensity is used to determine whether the access point's deployment location is currently populated with clients. |
| Shutdown WLAN Radio at Low Limit of Light Threshold | Select this option to power off the AP 8132's radio's fall below the set threshold. If enabled, select*All* (both AP 8132 radios), *radio-1* or *radio-2*. |
| Low Limit of Light Threshold | Set the low threshold limit (from 0 - 1,000 lux) to determine whether the lighting is off in the AP 8132's deployment location. The default is 100. |
| High Limit of Light Threshold | Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the AP 8132's deployment location. The default is 500. |

3 Enable or disable the following AP 8132 Environmental Sensors:

| | |
|---|---|
| Enable Temperature Sensor | Select this option to enable the module's temperature sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default. |
| Enable Motion Sensor | Select this option to enable the module's motion sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default. |
| Enable Humidity Sensor | Select this option to enable the module's humidity sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default. |

4 Define or override the following Shared Configuration settings:

| | |
|---|---|
| Polling Interval for All Sensors | Set an interval in either *Seconds* (1 - 100) or *Minutes* (1 - 2) for the time between environmental polling transmissions (both light and environment). The default setting is 5 seconds. |

5 Select **OK** to save the changes made to the environmental sensor screen. Select **Reset** to revert to the last saved configuration.

## Advanced Profile Configuration

An access point profile's advanced configuration is comprised of defining connected client load balance settings, a MINT protocol configuration and miscellaneous settings (NAS ID, access point LEDs and RF Domain Manager).

### *Client Load Balancing Configuration*

Set the ratios and calculation values used by access points to distribute client loads both among neighbor devices and the 2.4 and 5 GHz radio bands.

To define or override client load balance algorithms for access points:

1 Go to **Configuration → Devices → System Profiles**.

A list of default and user-created profiles is displayed.

2 Select a target profile from the displayed list.

The selected profile's configuration menu is displayed.

3 Expand the **Advanced** menu and select **Client Load Balancing**.

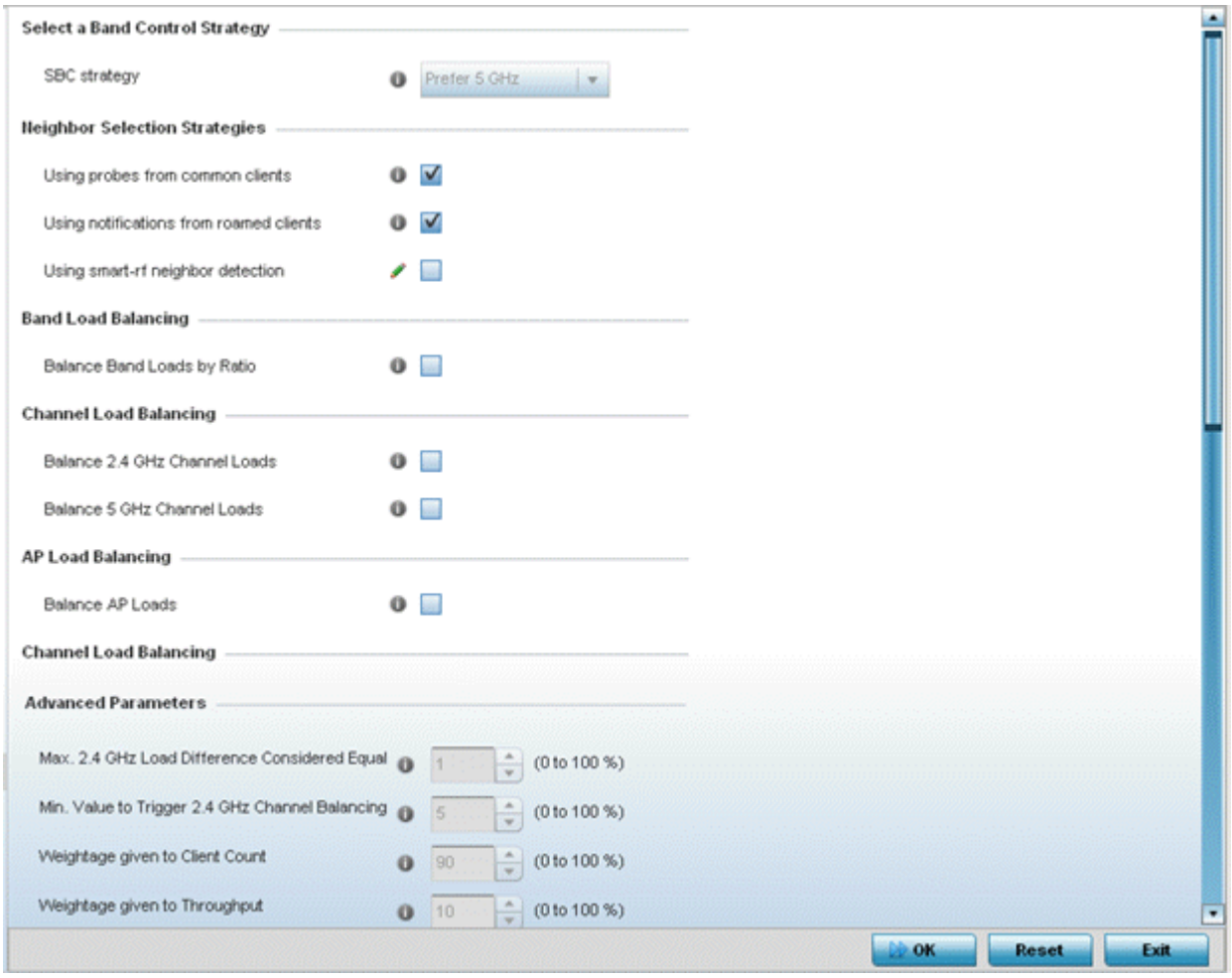



**Figure 118: Profile Overrides - Client Load Balancing Screen**

4 Use the Group ID field to define a group ID of up to 32 characters to differentiate this profile from others with similar configurations.

5 Use the **SBC strategy** drop-down menu to determine how band steering is conducted.

Options include **`Prefer 5GHz`**, **`Prefer 2.4 GHz`** and **`distribute-by-ratio`**. The default value is **`Prefer 5GHz`**.

Band steering directs 5 GHz-capable clients to that band. When an access point hears a request from a client to associate on both the 2.4 GHz and 5 GHz bands, it knows the client is capable of operation in 5 GHz. Band steering steers the client by responding only to the 5 GHz association request and not the 2.4 GHz request. The client associates in the 5 GHz band only.

6 Set the following **Neighbor Selection Strategies**:

| | |
|---|---|
| Using Probes from common clients | Select this option to select neighbors (peer devices) using probes from common clients. This option is enabled by default. |
| Using Notifications from roamed clients | Select this option to select neighbors (peer devices) using roam notifications from roamed clients. This option is enabled by default. |
| Using smart-rf neighbor detection | Select this option to select neighbors (peer devices) using the Smart RF neighbor detection algorithm. This option is enabled by default. |

7 Enable **Balance Band Loads by Ratio**, in the **Band Load Balancing** field, to distribute an access point's client traffic load across both the 2.4 and 5 GHz radio bands.

8 Configure the following **Channel Load Balancing** settings:

| | |
|---|---|
| Balance 2.4 GHz Channel Loads | Select this option to balance the access point's 2.4GHz radio load across the channels supported in the country of deployment. This can prevent congestion on the 2.4GHz radio if a channel is overutilized. |
| Balance 5 GHz Channel Loads | Select this option to balance the access point's 5GHz radio load across the channels supported in the country of deployment. This can prevent congestion on the 5GHz radio if a channel is overutilized. |

9 Enable **Balance AP Loads**, in the **AP Load Balancing** field, to distribute client traffic evenly among neighbor access points.

AP loads are balanced by assigning a ratio to both the 2.4 and 5GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 or 5 GHz band.

10 Set the following **Band Control** values:

| | |
|---|---|
| Max. Band Load Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 and 5GHz radio band load balances on this access point. The default setting is 10%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing 2.4 and 5 GHz load balances on this access point. |
| Band Ratio (2.4 GHz) | Set a loading ratio (between 0 - 10) the access point 2.4 GHz radio uses in respect to radio traffic load on the 2.4 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz radio band. The higher this value is set, the greater the weight assigned to radio traffic load on the 2.4 GHz radio band. The default setting is 1. |
| Band Ratio (5 GHz) | Set a loading ratio (between 0 - 10) the access point 5 GHz radio uses in respect to radio traffic load on the 5 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 5 GHz radio band. The higher this value is set, the greater the weight assigned to radio traffic load on the 5 GHz radio band. The default setting is 1. |
| 5 GHz load at which both bands enabled | Set a load percentage (between 0 - 100) that enables the other band (2.4 GHz) to share load with the current band. |
| 2.4 GHz load at which both bands enabled | Set a load percentage (between 0 - 100) that enables the other band (5 GHz) to share load with the current band. |

11 Define the following **Neighbor Selection** settings:

| | |
|---|---|
| Minimal signal strength for common clients | Set the minimum signal strength require to learn about neighbors from clients that are common with the neighbor access point. |
| Minimum number of clients seen | Set the minimum number of common clients seen before the neighbor is learned. |

| | |
|---|---|
| Max confirmed neighbors | Set the maximum number of learned neighbors stored at this device. |
| Minimum signal strength for smart-rf neighbors | Set the minimum signal strength of neighbor devices that are learned through Smart RF before being recognized as neighbors. |

12 Set the following **Advanced** parameters in the **Channel Load Balancing** section:

| | |
|---|---|
| Max. 2.4 GHz Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points. |
| Min. Value to Trigger 2.4 Ghz Channel Balancing | Define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 2.4GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70%. |
| Weightage given to Client Count | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Increase this value if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%. |
| Weightage given to Throughput | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Increase this value if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%. |
| Max. 5 GHz Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing 5 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points. |
| Min. Value to Trigger 5 Ghz Channel Balancing | Define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 5GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70%. |
| Weightage given to Client Count | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Increase this value if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%. |
| Weightage given to Throughput | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%. |

13 Define the following **AP Load Balancing** settings:

| | |
|---|---|
| Min. Value to Trigger Load Balancing | Set the access point radio threshold value (from 0 - 100%) used to initiate load balancing across other access point radios. When this radio load exceeds the defined threshold, load balancing is initiated. The default is 70%. |
| Max. AP Load Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing access point radio load balances. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing access point radio load balances. |

| | |
|---|---|
| Weightage given to Client Count | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Increase this value if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%. |
| Weightage given to Throughout | Assign a weight (between 0 - 100) the access point uses to prioritize throughput in the access point load calculation. Increase this value if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%. |

14 Click **OK** to save the changes made to the profile's advanced client load balance configuration

Click **Reset** to revert to the last saved configuration.

*Settings Configuration*

MiNT provides the means to secure profile communications at the transport layer. Using MiNT, a device can be configured to only communicate with other authorized (MiNT enabled) devices. Keys can also be generated externally using any application (like openssl). These keys must be present on the device managing the domain for key signing to be integrated with the UI. A device needing to communicate with another first negotiates a security context with that device.

The security context contains the transient keys used for encryption and authentication. A secure network requires users to know about certificates and PKI. However, administrators do not need to define security parameters for Access Points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MiNT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed

To define or override a profile's MiNT configuration:

1 Go to **Configuration → Devices → System Profiles**.

A list of default and user-created profiles is displayed.

2 Select a target profile from the displayed list.

The selected profile's configuration menu is displayed.

3 Expand Advanced tab and select **MiNT Protocol**.

The Settings tab displays by default.

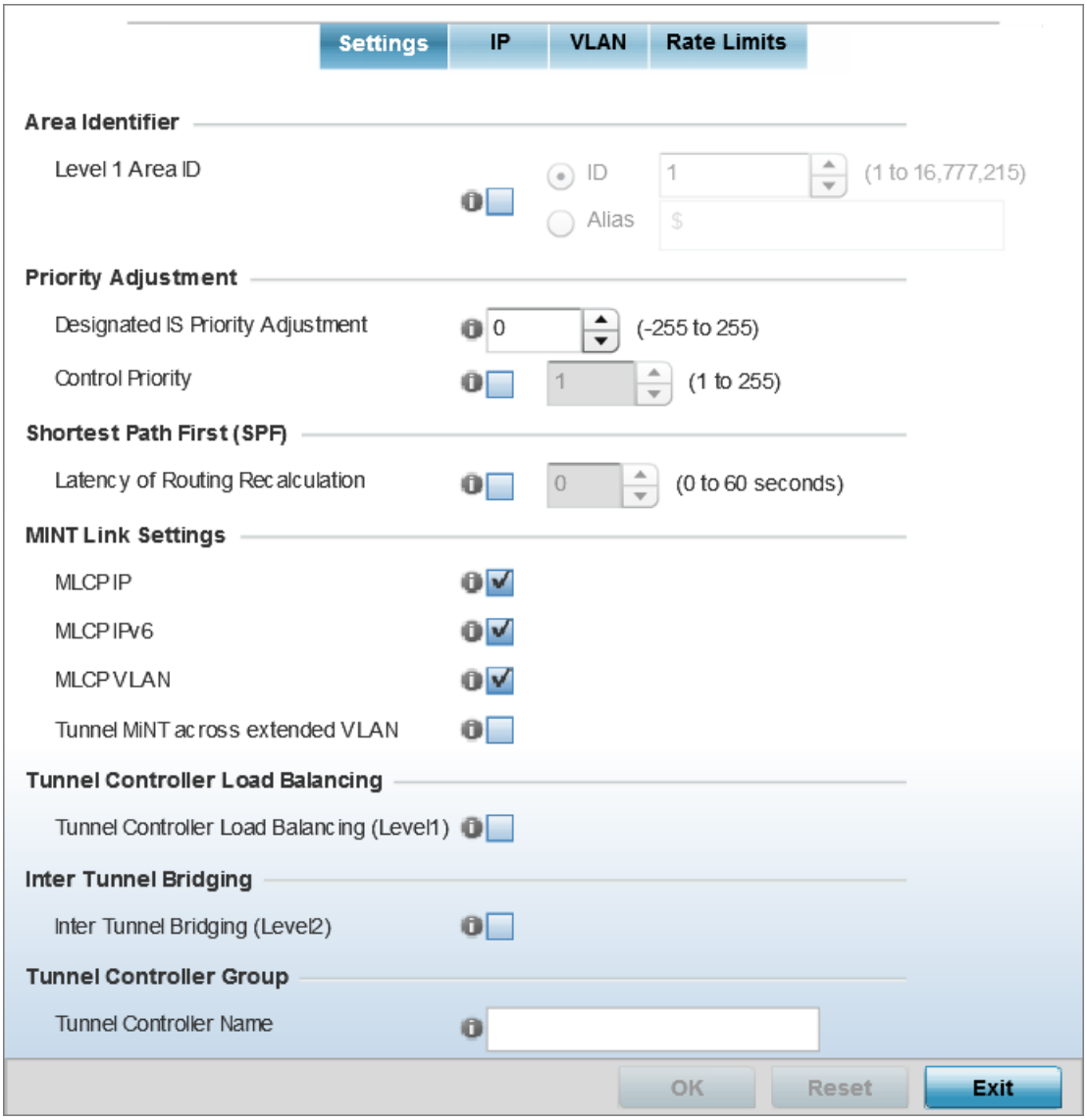



**Figure 119: Advanced Profile Overrides MiNT Screen - Settings Tab**

4 Refer to the Area Identifier field to define or override the Level 1 and Level 2 Area IDs used by the profile's MiNT configuration.

| | |
|---|---|
| Level 1 Area ID | Select this option to enable a spinner control for setting the Level 1 Area ID from 1 - 16,777,215. The default value is disabled. Alternatively, provide an alias by selecting the **`Alias`** option and adding the alias name to this field. |

5 Define or override the following **Priority Adjustments** settings in respect to devices supported by the profile:

| | |
|---|---|
| Designated IS Priority Adjustment | Use the spinner control to set a Designated IS Priority Adjustment setting from -255 - +255. This is the value added to the base level DIS priority to influence the Designated IS (DIS) election. A value of +1 or greater increases DISiness. The default setting is 0. |

6 Select the **Latency of Routing Recalculation** option, in the Shortest Path First (SPF) field, to enable the spinner control used for defining or overriding a latency period (from 0 - 60 seconds).

The option is disabled by default.

7 Define or override the following MiNT Link Settings in respect to devices supported by the profile:

| | |
|---|---|
| MLCP IP | Select this option to enable MLCP *(MiNT Link Creation Protocol)* by IP Address. MLCP is used to create a UDP/IP link from the device to a neighbor.<br>The neighboring device can be another AP. |
| MLCP IPv6 | Select this option to enable *MiNT Link Creation Protocol* (MLCP) by IPv6 Address. MLCP by IPv6 is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a virtual controller; it can be an standalone access point. |
| MLCP VLAN | Select this option to enable MiNT MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor.<br>The neighboring device can be another AP. |
| Tunnel MiNT across extended VLAN | Select this option to tunnel MiNT protocol packets across an extended VLAN. This setting is disabled by default. |

8 Select **Tunnel Controller Load Balancing (Level 1)** to enable load balancing through a WLAN tunnel controller.

This setting is disabled by default.

9 Select **Inter Tunnel Bridging (Level 2)** to enable inter tunnel bridging.

This setting is disabled by default.

10 Enter a 64-character maximum **Tunnel Controller Name** for this tunneled-WLAN-controller interface.

11 Define the group name of clustered tunnel controllers in the Preferred Tunnel Controller Name field.

12 Click **OK** to save the changes made to the MiNT protocol configuration.

Click **Reset** to revert to the last saved configuration.

### IP Configuration

1 Select the **IP** tab to display the link IP network address information shared by the devices managed by the MiNT configuration.

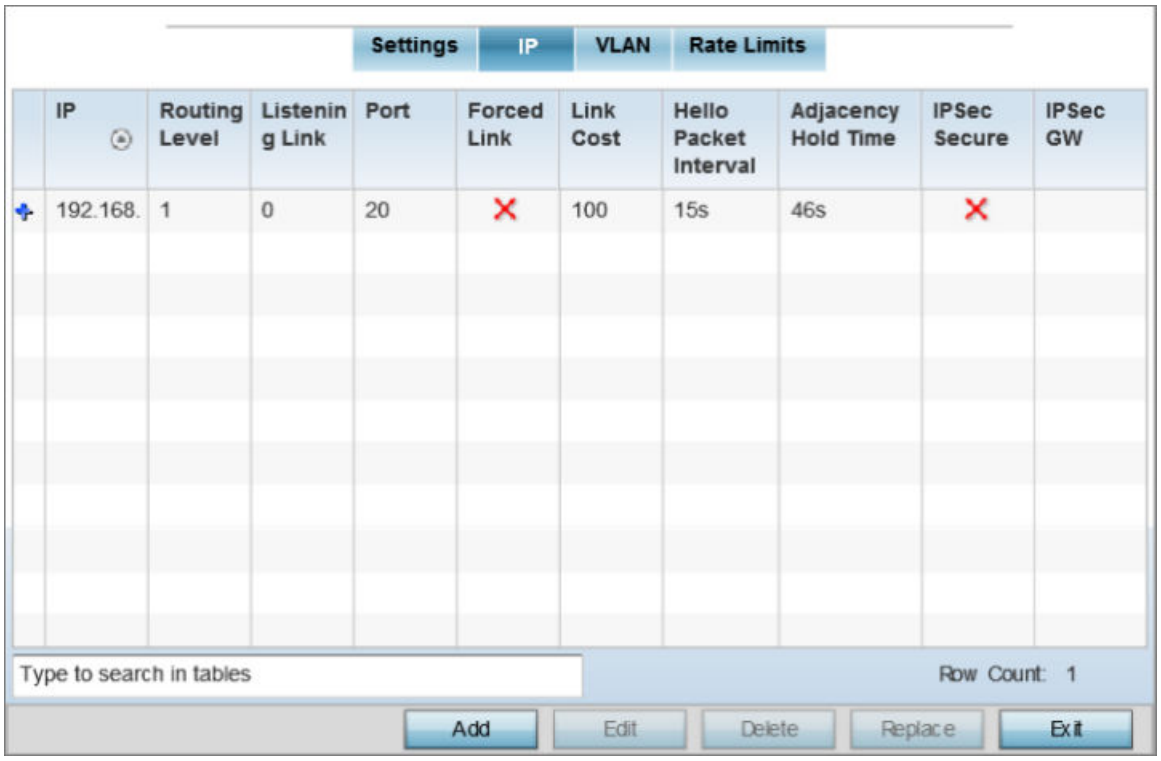



**Figure 120: Advanced Profile Overrides MiNT Screen - IP Tab**

2 Review the existing MiNT IP settings. The IP tab displays the IP address, Routing Level, Listening Link, Port, Forced Link, Link Cost, Hello Packet Interval, Adjacency Hold Time, IPSec Secure, and IPSec GW information that managed devices use to communicate securely with each other.

3 Click **Add** to create a new link IP configuration or **Edit** to override an existing configuration.

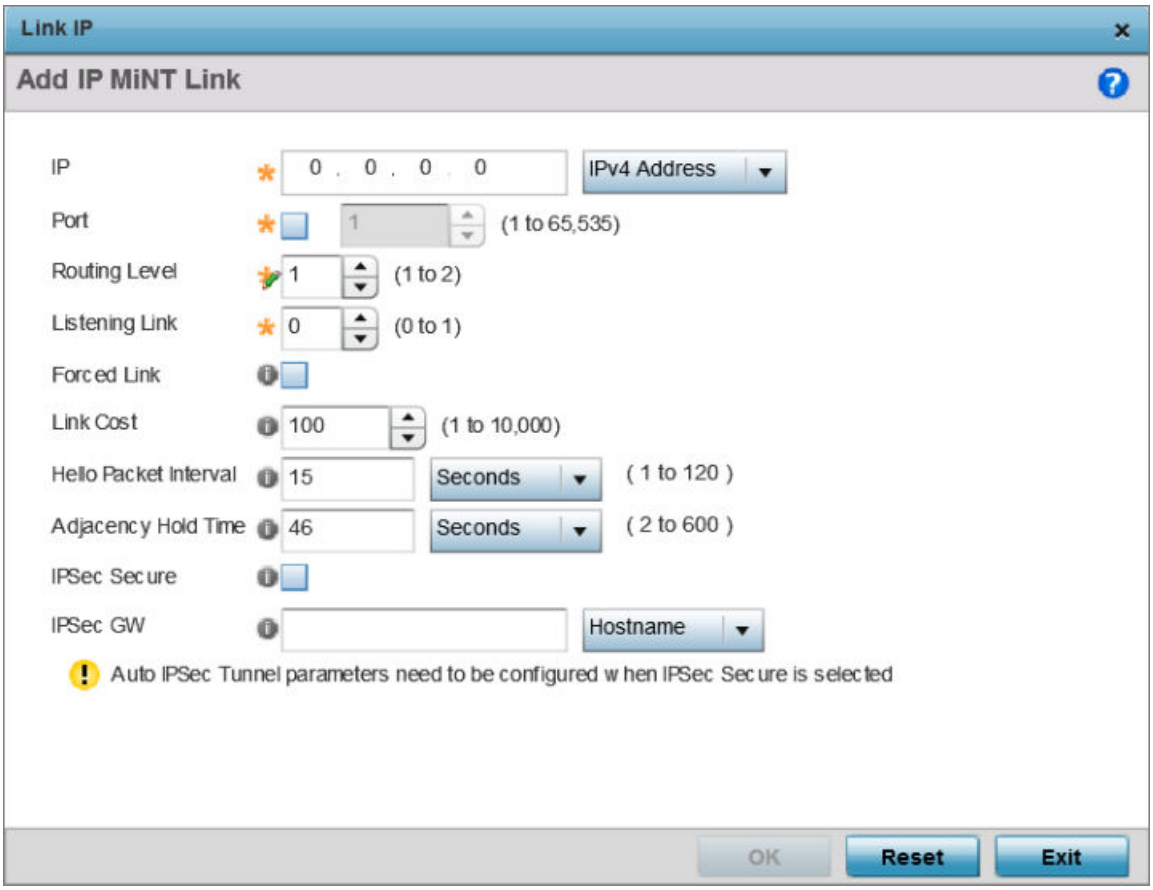



**Figure 121: Advanced Profile Overrides MiNT Screen - Add IP MiNT Link**

4 Set the following Link IP parameters for the MiNT network address configuration:

| | |
|---|---|
| IP | Define or override the IP address used by peer access points for interoperation when supporting the MiNT protocol. |
| Port | To specify a custom port for MiNT links, select this option and use the spinner control to define or override the port number from 1 - 65,535. |
| Routing Level | Define or override a routing level of either 1 or 2. |
| Listening Link | Specify a listening link of either 0 or 1. UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and does not scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted. |
| Forced Link | Select this option to specify the MiNT link as a forced link. This setting is disabled by default. |
| Link Cost | Define or override a link cost from 1 - 10,000. The default value is 100. |
| Hello Packet Interval | Set or override an interval in either seconds (1 - 120) or minutes (1 - 2) for the transmission of hello packets. The default interval is 15 seconds. |
| Adjacency Hold Time | Set or override a hold time interval in either seconds (2 - 600) or minutes (1 - 10) for the transmission of hello packets. The default interval is 46 seconds. |

| | |
|---|---|
| IPSec Secure | Select this option to use a secure link for IPSec traffic. This setting is disabled by default. When this option is enabled, both the header and the traffic payload are encrypted. |
| IPSec GW | Define either an IP address or hostname for the IPSec gateway. |

5 Click **OK** to save the changes made to the MiNT protocol network address configuration.

Click **Reset** to revert to the last saved configuration.

### VLAN Configuration

1 Select the **VLAN** tab to display the link IP VLAN information shared by the access points managed by the MiNT configuration.

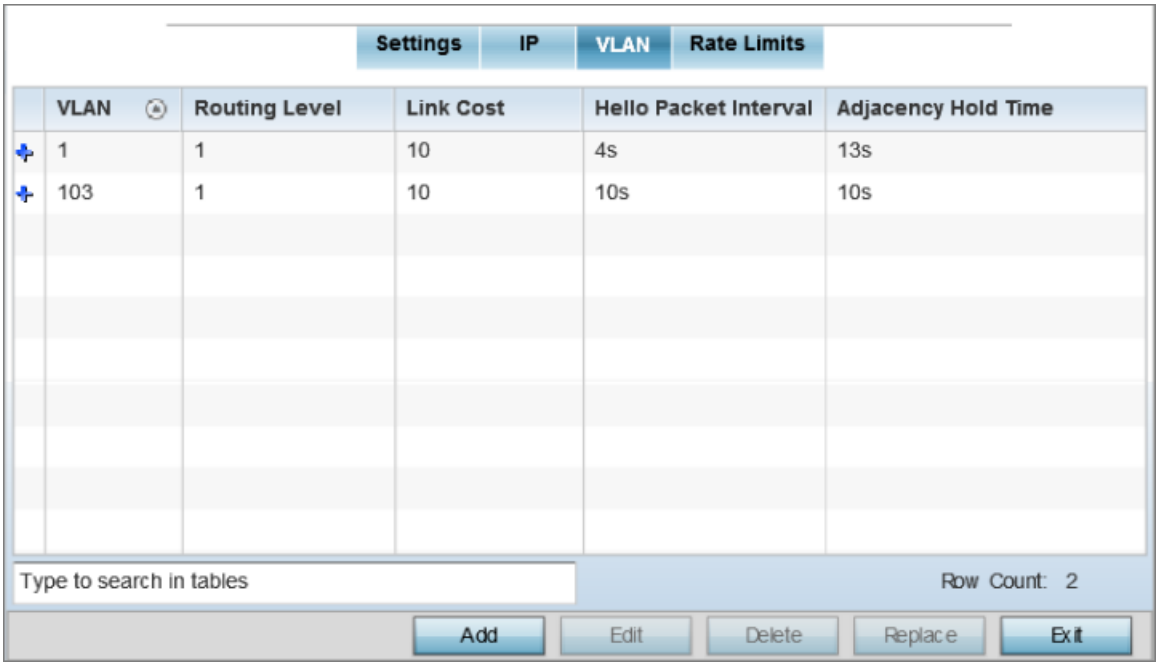



**Figure 122: Advanced Profile Overrides MiNT Screen - VLAN Tab**

2 Review existing VLAN configuration.

The VLAN tab displays the VLAN, Routing Level, Link Cost, Hello Packet Interval, and Adjacency Hold Time managed devices use to communicate securely with each another.

3 Click **Add** to create a new VLAN link configuration or **Edit** to override an existing configuration.

Note

If creating a mesh link between two access points in Standalone AP mode, you'll need to ensure a VLAN is available to provide the necessary MiNT link between the two Standalone APs.

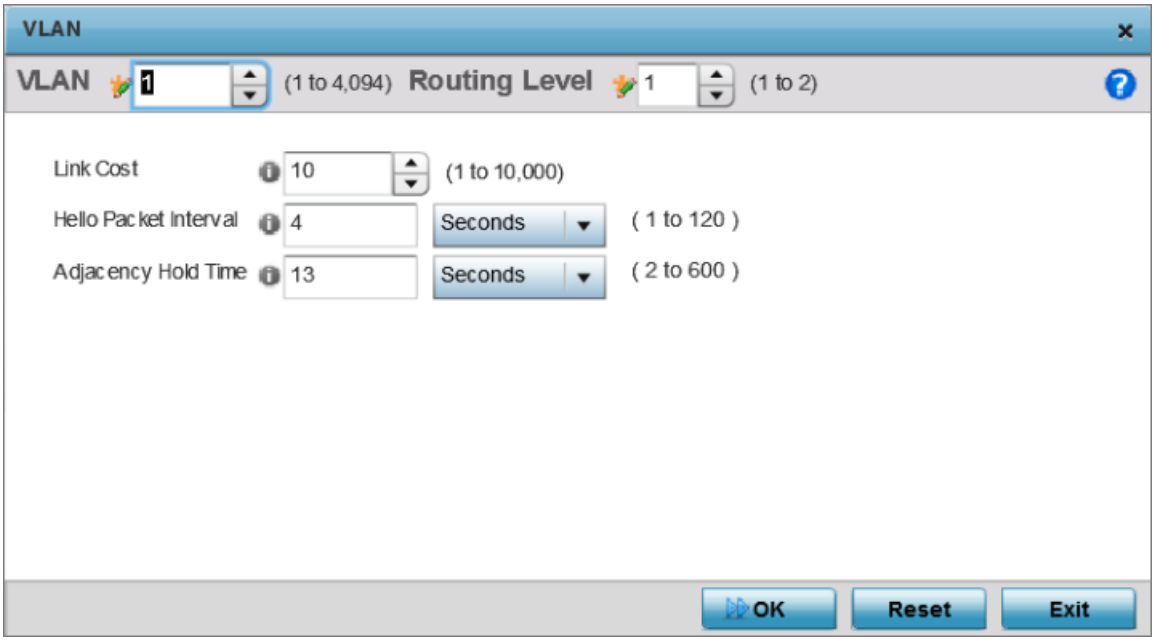



**Figure 123: Advanced Profile Overrides MiNT Screen - Add/Edit VLAN**

4 Set the following VLAN parameters for the MiNT configuration:

| | |
|---|---|
| VLAN | Define a VLAN ID from 1 - 4094 used by peer controllers for interoperation when supporting the MiNT protocol |
| Routing Level | Define or override a routing level of either 1 or 2. |
| Link Cost | Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 10. |
| Hello Packet Interval | Set or override an interval in either seconds (1 - 120) or minutes (1 - 2) for the transmission of hello packets. The default interval is 4 seconds. |
| Adjacency Hold Time | Set or override a hold time interval in either seconds (2 - 600) or minutes (1 - 10) for the transmission of hello packets. The default interval is 13 seconds. |

5 Click **OK** to save the changes made to the MiNT protocol configuration.

Click **Reset** to revert to the last saved configuration.

### Rate Limit Configuration

1 Select the **Rate Limits** tab.

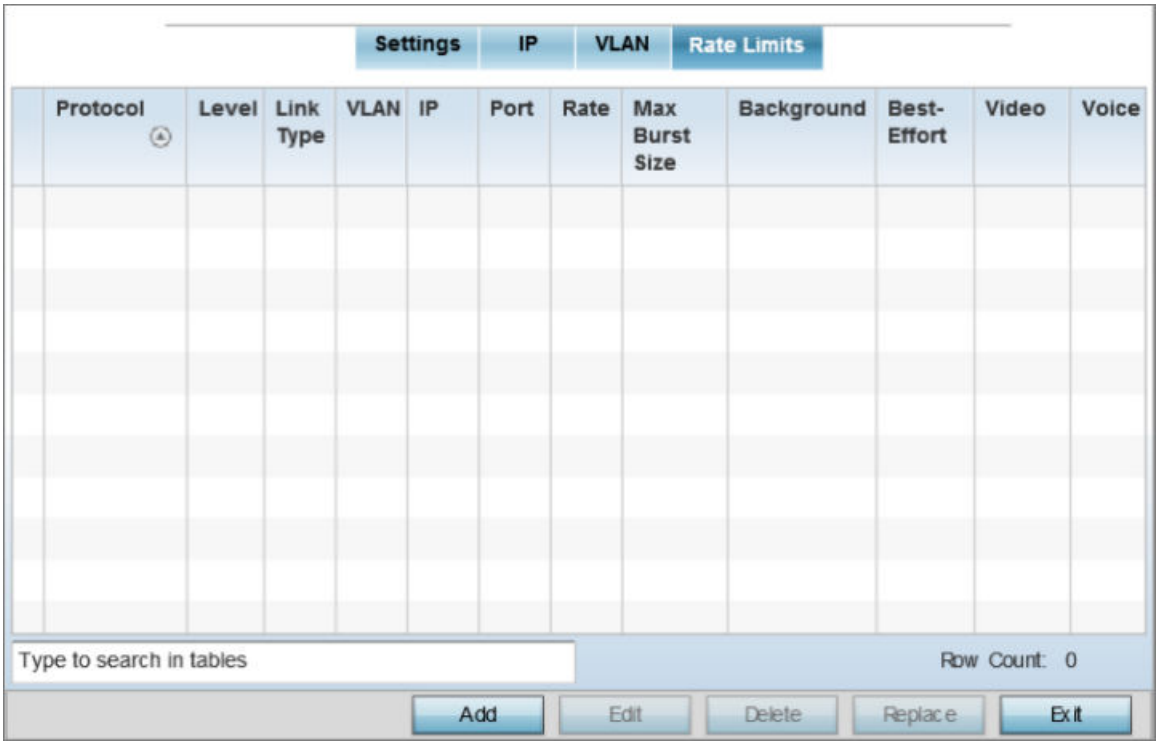



**Figure 124: Advanced Profile Overrides MiNT Screen - Rate Limits Tab**

2 Review existing Rate Limit configuration details.

The Rate Limits tab displays the Protocol, Level, Link Type, VLAN, IP, Port, Rate, Max Burst Size, Background, Best-Effort, Video, and Voice rate limiting parameters for each of the configured devices.

Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices, or malicious software such as a worm or virus that has infected on one or more devices. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform, or access point are applied. An administrator can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream). Existing rate limit configurations display along with their virtual connection protocols and data traffic QoS customizations.

3 Click **Add** to create a new MiNT rate limiting configuration or **Edit** to override an existing configuration.

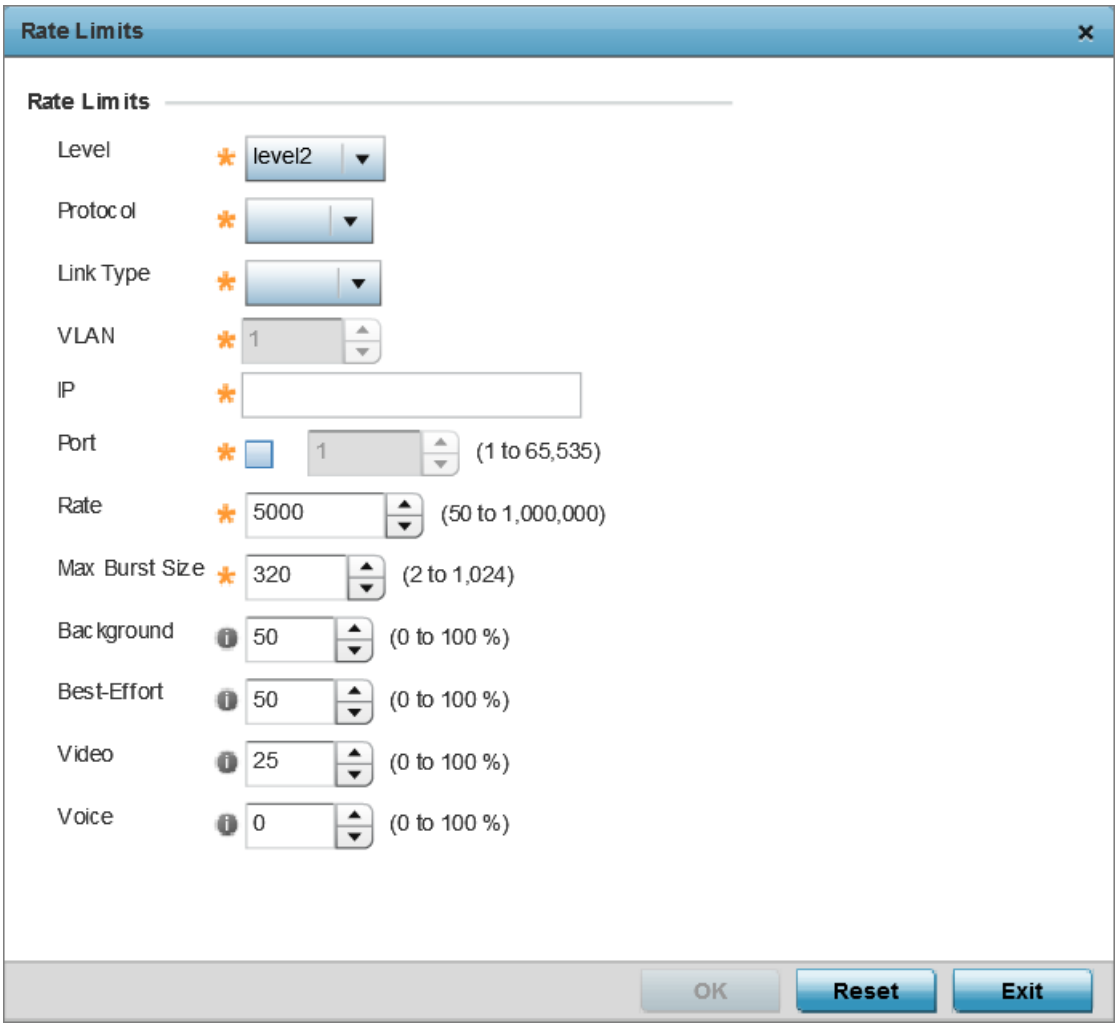



**Figure 125: Advanced Profile Overrides MiNT Screen - Add/Edit Rate Limit**

4 Set the following Rate Limits to complete the MiNT configuration:

| | |
|---|---|
| Level | Select **`level2`** to apply rate limiting for all links on level 2. |
| Protocol | Select either **`mlcp`** or **`link`** as this configuration's rate limit protocol. *MiNT Link Creation Protocol* (MLCP) creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform; it can be an access point with a path to the controller or service platform. Select **`link`** to rate limit using statically configured MiNT links. |
| Link Type | Select either **`VLAN`**, to configure a rate limit configuration on a specific virtual LAN, or **`IP`** to set rate limits on a static IP address/port configuration. |
| VLAN | When **Protocol** is set to **`link`** and **Link Type** is set to **`VLAN`**, select a virtual LAN from 1 - 4094 to refine the rate limiting configuration to a specific VLAN. |
| IP | When **Protocol** is set to **`link`** and **Link Type** is set to **`VLAN`**, enter the IP address as the network target for rate limiting. |

| | |
|---|---|
| Port | When **Protocol** is set to **link** and **Link Type** is set to **VLAN**, set the virtual port (1 - 65,535) used for rate limiting traffic. |
| Rate | Define a rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps. |
| Max Burst Size | Set the maximum burst size from 0 - 1024 kb. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes. |
| Background | Configure the random early detection threshold (as a percentage) for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%. |
| Best-Effort | Configure the random early detection threshold (as a percentage) for low priority best effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 50%. |
| Video | Configure the random early detection threshold (as a percentage) for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 25%. |
| Voice | Configure the random early detection threshold (as a percentage) for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 0%. |

5 Click **OK** to save the changes made to the MiNT protocol rate limit configuration.
Click **Reset** to revert to the last saved configuration.

*Miscellaneous Configuration*

Refer to the advanced profile's Miscellaneous menu item to set or override a profile's NAS configuration. The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port. Each profile is matched to a username representing a physical port.

Access point LED behavior and RF Domain management can also be defined from the Miscellaneous screen.

To define or override a profile's miscellaneous configuration attributes:

1 Go to **Configuration → Devices → System Profiles**.
A list of default and user-created profiles is displayed.

2 Select a target profile from the displayed list.

The selected profile's configuration menu is displayed.

3 Expand the **Advanced** menu and select **Miscellaneous**.

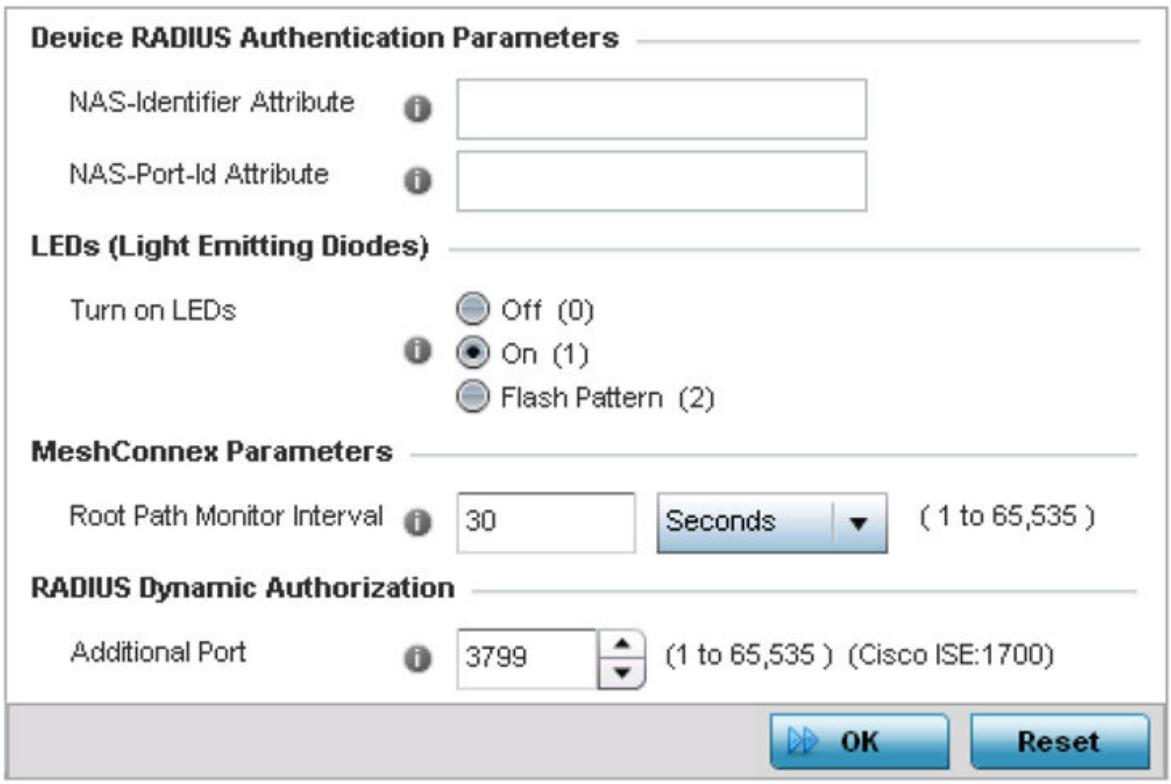



**Figure 126: Advanced Profile Overrides - Miscellaneous Screen**

4 Set a **NAS-Identifier Attribute** up to 253 characters in length.

This is the RADIUS NAS-Identifier attribute that typically identifies where a RADIUS message originates.

5 Set a **NAS-Port-Id Attribute** up to 253 characters in length.

This is the RADIUS NAS port ID attribute which identifies the device port where a RADIUS message originates.

6 Select **Turn on LEDs** to enable an adopted access point's LEDs.

This feature is enabled by default.

7 Select **Flash Pattern(2)** to enable the access point to blink in a manner different from its operational LED behavior.

Enabling this option allows an administrator to validate that the access point has received its configuration from its managing controller during staging. In the staging process, the administrator adopts the access point to a staging controller to get an initial configuration before the access point is deployed at its intended location. Once the access point has received its initial configuration, its LED blinks in a unique pattern to indicate the initial configuration is complete.

8 Use the drop-down menu to configure the access point's **Meshpoint Behavior**.

This field configures the access point's mobility behavior. The default is **`External (fixed)`**, which means that the mesh point is fixed. The value **`vehicle-mounted`** means that the mesh point is mobile. This feature is available only on an AP 7161 model access point.

9 Select **Capable**, in the RF Domain Manager section, to designate this specific device as being the RF Domain manager for a particular RF Domain.

The default value is enabled.

10 Select **Priority**, in the **RF Domain Manager** section, to set a priority value for this specific profile managed device. O

Once enabled, use the spinner control to set a device priority between 1 - 255. The higher the number you select, the higher the priority in the RF Domain manager election process.

11 Use **Root Path Monitor Interval** to configure the interval to monitor the path to the root node.

12 Set the **Additional Port** value, in the **RADIUS Dynamic Authorization** section, to enable a Cisco ISE *(Identity Services Engine)* (AAA) *(Authentication, Authorization and Accounting)* server to dynamically authenticate a client.

Set this value to 1700. The allowed port range is 1 to 65,535.

When a client device requests access to the network, the Cisco ISE RADIUS server presents the client with a URL where a device's compliance is checked for definition file validity (this form of file validity checking is called *posture*). The check verifies, for example, that the device's anti-virus or anti-spyware software is valid. If the device complies, it is allowed access to the network.

13 Click **OK** to save the changes made to the profile's advanced miscellaneous configuration.

Click **Reset** to revert to the last saved configuration.

## Managing Virtual Controllers

Access points set to function as Standalone APs can be re-defined as Virtual Controllers as required, and Virtual Controllers can reverted back to Standalone APs. Consider setting the access point to a Virtual Controller when more than one access points (of the same model) are deployed are require management from a centralized access point. Up to 64 Dependent mode access points can be connected to, and managed by, a single Virtual Controller AP of the same model.

Note

If designating the access point as a Standalone AP, it is recommended that the access point's UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile, while the UI only provides one per access point model. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.

Note

The recommended way to administer a network populated by numerous access points is to configure them directly from the designated Virtual Controller AP. If an access point's configuration requires an exception from the Virtual Controller AP's assigned profile configuration the administrator should apply a Device Override to change just that access point's configuration.

Note

WiNG 5.9.X model access points support heterogeneous virtual controller adoption. For more information on the supported adoption hierarchy, see Heterogeneous AP Management on page 9.

Note

The WiNG 7.1 AP505 and AP510 model access points can be deployed as virtual controllers. However, heterogeneous adoption is not supported. An AP505 can only adopt another AP505. And an AP510 can only adopt another AP510 model access point.

To define a Standalone AP as a Virtual Controller AP:

1 Select **Configuration → Devices → Virtual Controller**.

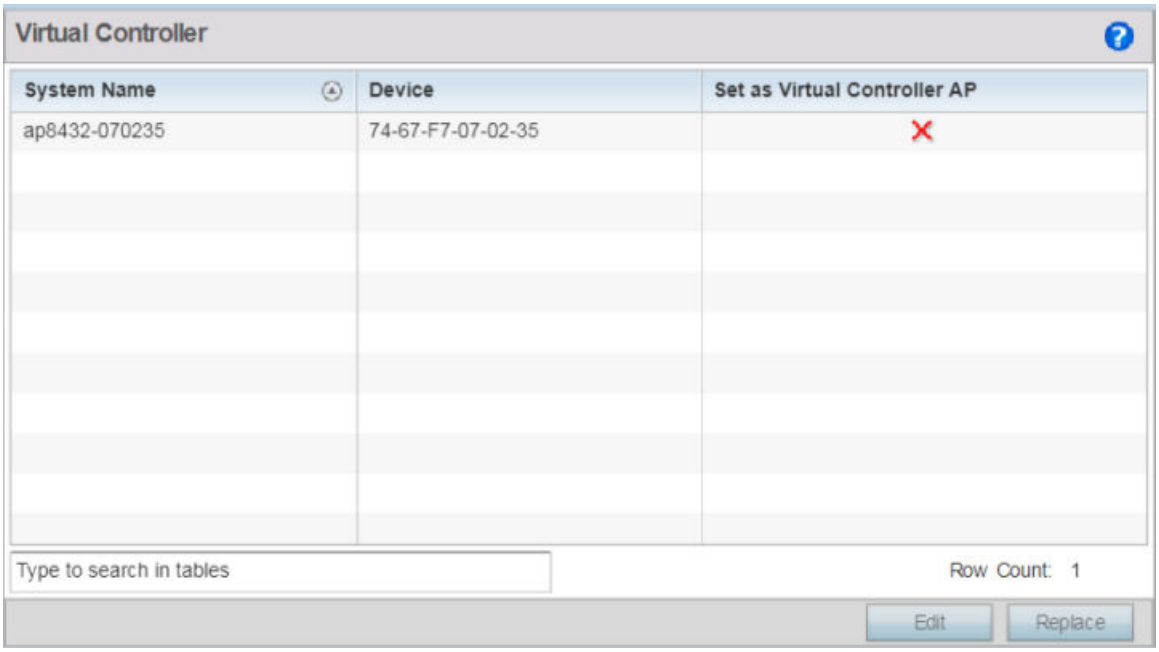



**Figure 127: Virtual Controller Screen**

2 This Virtual Controller screen lists all peer access points within this Virtual Controller's radio coverage area. Each listed access point is listed by its assigned System Name, MAC Address and Virtual Controller designation.

3 Either select an access point from those displayed and select **Edit**, or use the device browser in the lower left-hand side of the UI to select an access point.

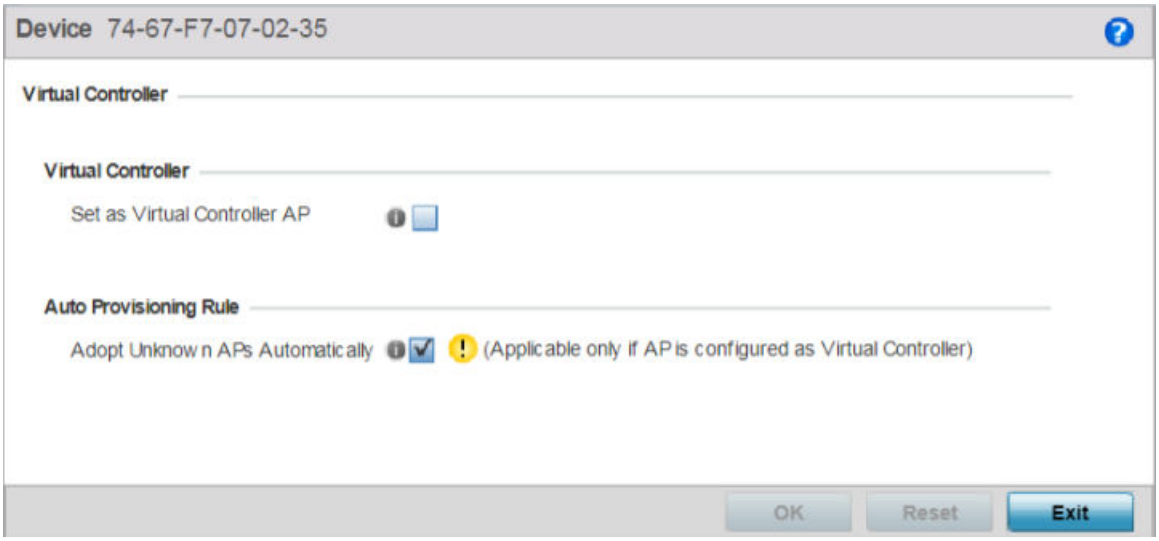



**Figure 128: Managing Virtual Controller - AP Designation Screen**

4 Select the **Set as Virtual Controller AP** radio button to change the selected access point's designation from Standalone to Virtual Controller AP. Remember, only one Virtual Controller can manage (up to) 64 access points of the same model. Thus, an administrator should take care to change the designation of a Virtual Controller AP to Standalone AP to compensate for a new Virtual Controller AP designation.

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

Click **Reset** to revert to the last saved configuration. Select **Delete** to remove obsolete rows as needed.

## Device Overrides

Devices within the access point managed network can have an override configuration defined and applied. New devices can also have an override configuration defined and applied once.

Note

The best way to administer a network populated by numerous access points is to configure them directly from the designated Virtual Controller AP. If an access point's configuration requires an exception from the Virtual Controller AP's assigned profile configuration the administrator should apply a Device Override to change just that access point's configuration. For more information on access point's Virtual Controller AP assigned configuration profile, see System Profile Configuration on page 72.

Refer to the following configuration overrides, applicable to devices within a access point managed network:

- Basic Configuration on page 298
- Certificates Configuration on page 300
- Wired 802.1x Configuration on page 317

- RF Domain Overrides on page 319
- Device Profile Overrides on page 322

## Basic Configuration

Applying a basic configuration override to a device entails changing (overriding) the device's system name, deployment area, building floor and system clock.

When a device is initially deployed, it requires several basic configuration parameters be set and its deployment location defined. Additionally, the number of permitted licenses needs to be accessed to determine whether new devices can be adopted (if in Virtual Controller AP mode).

To override a managed device's basic configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays, with the Basic configuration screen selected by default.

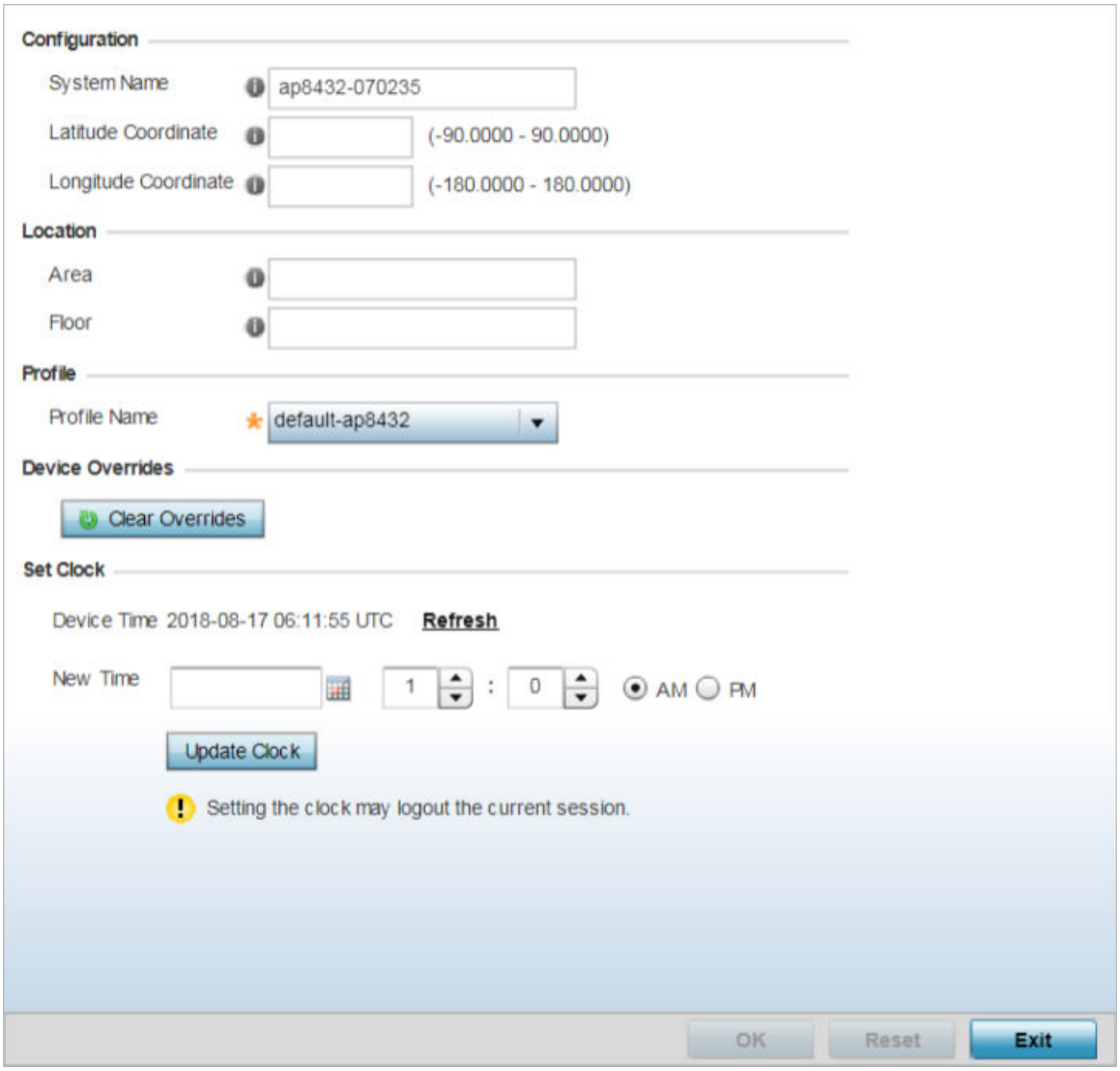



**Figure 129: Device Overrides - Basic Configuration Screen**

3 In the Configuration field, set the following settings for the selected device:

| | |
|---|---|
| System Name | Provide the selected device a system name up to 64 characters in length. This is the device name that appears within the RF Domain or Profile the access point supports and is identified by. |
| Latitude Coordinate | Optionally provide the latitude coordinate where the device is located. The valid value for this field is in the range -90.0000 degrees to +90.0000 degrees. When provided, this enables the device to be mapped on the geolocation map. |
| Longitude Coordinate | Optionally provide the longitude coordinate where the device is located. The valid value for this field is in the range -180.0000 degrees to +180.0000 degrees. When provided, this enables the device to be mapped on the geolocation map. |

4 In the Location field, set the following device deployment related information:

| | |
|---|---|
| Area | Assign the access point an Area representative of the location the access point is physically deployed. The name cannot exceed 64 characters. Assigning an area is helpful when grouping access points in profiles, as access points in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location. |
| Floor | Assign the target access point a building Floor name representative of the location the access point was physically deployed. The name cannot exceed 64 characters. Assigning a building floor name is helpful when grouping devices in profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location. |

5 In the Profile field, use the **Profile Name** drop-down menu to override the profile applied to the device.

6 Refer to the Device Overrides field to assess whether overrides have been applied to the device's configuration.

Use the **Clear Overrides** button to clear all device overrides and reset the configuration to its default values.

7 In the Set Clock field, update the system time if needed.

a Refer to the Device Time parameter to assess the device's current time.

If the device's time has not been set, the device time is displayed as unavailable. Select **Refresh** to update the device's system time.

b Use the New Time parameter to set the *calendar day*, *hour* and *minute*. Use the **AM** and **PM** radio buttons to refine whether the updated time is for the *AM* or *PM* respectively. This time can be synchronized with the use of an external NTP resource.

c Click **Update Clock** to commit the updated time to the device.

8 Click **OK** to save the basic configuration changes.

Click **Reset** to revert to the last saved configuration.

## Certificates Configuration

A certificate links identity information with a public key enclosed in the certificate.

A CA *(certificate authority)* is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its Trusted Root Library so it can trust certificates signed by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. SSH *(Secure Shell)* public key authentication can be used by a client to access resources, if properly configured. A RSA key pair must be generated on the client. The public portion of the key pair resides with the licensed device, while the private portion remains on the client.

The certificate configuration used by an access point managed device can be changed (overridden) as changes in security credentials require modification in the management of the device.

To override a managed device's certificate configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays, with the Basic configuration screen selected by default.

3 Select **Certificates**.

The certificates configuration screen displays.

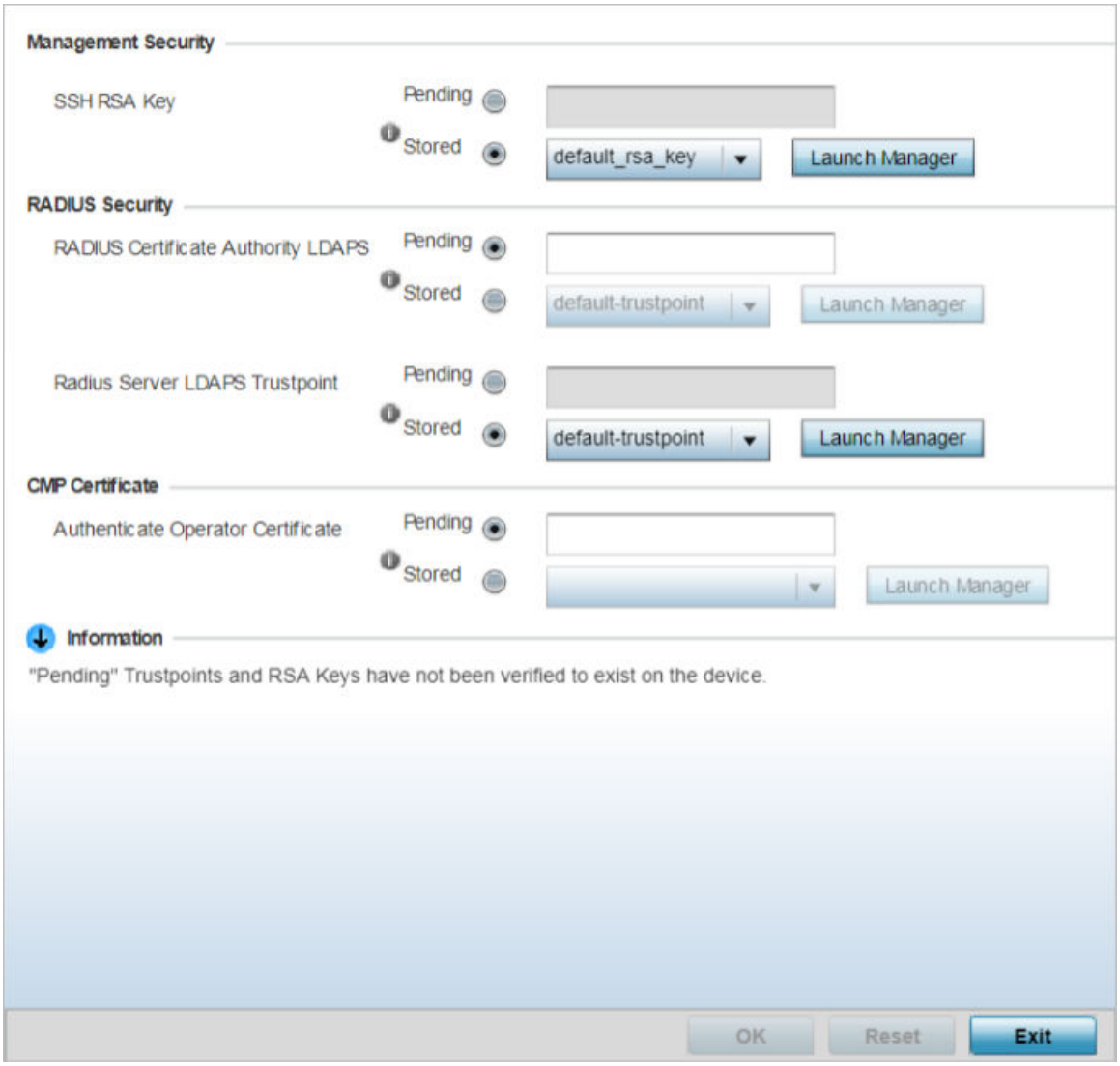



**Figure 130: Device Overrides - Certificates Configuration Screen**

4 In the Management Security field, set the following configurations:

| | |
|---|---|
| HTTPS Trustpoint | Either use the default-trustpoint or select the Stored radio button to enable a drop-down menu where an existing certificate/trustpoint can be leveraged. To leverage an existing device certificate for use with this target device, select the Launch Manager button. For more information, see Manage Certificates on page 303. |
| SSH RSA Key | Either use the default_rsa_key or select the Stored radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing key, select the Launch Manager button. For more information, see RSA Key Management on page 308. |

5 Set the RADIUS Security certificate configuration. Select the **Stored** radio button to enable a drop-down menu where an existing certificate/trustpoint can be leveraged. To leverage an existing device certificate for use with this target device, select the **Launch Manager** button.

Pending trustpoints and RSA keys are typically not verified as existing on a device.

| | |
|---|---|
| RADIUS Certificate Authority | Either use the default-trustpoint or select the Stored radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the **Launch Manager** button. |
| RADIUS Server Certificate | Either use the default-trustpoint or select the Stored radio button to enable a drop-down menu where an existing certificate/trustpoint can be used. To leverage an existing trustpoint, select the **Launch Manager** button. |
| RADIUS Certificate Authority LDAPS | Either use the LDAP server default-trustpoint or select the Stored radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the **Launch Manager** button. |
| RADIUS Server LDAPS Trustpoints | Either use the LDAP server default-trustpoint or select the Stored radio button to enable a drop-down menu where an existing certificate/trustpoint can be used. To leverage an existing trustpoint, select the **Launch Manager** button. |

6 in the CMP Certificate field, use the **Authenticate Operator Certificate** to validate the operator's cross-certificate with the existing vendor certificate installed on the device.

Use the **Launch Manager** to view more information on the installed vendor certificates. For more information on managing vendor certificates, seeCrypto CMP Policy on page 685.

7 Select **OK** to save the changes made to the certificate configurations.

Selecting **Reset** reverts the screen to its last saved configuration.

For more information on the certification activities, refer to the following:

- Manage Certificates on page 303
- RSA Key Management on page 308
- Certificate Creation on page 313
- Generating a Certificate Signing Request on page 315

*Manage Certificates*

If you do not want to use an existing certificate or key with a selected device, an existing stored certificate can be leveraged from a different device. Device certificates can be imported and exported to a secure remote location for archive and retrieval as required for application to other devices.

To configure trustpoints for use with certificates:

1 Select **Launch Manager** from the SSH RSA Key section.

The Certificate Management screen displays, with the Manage Certificates tab selected by default. This screen displays all existing trustpoints.

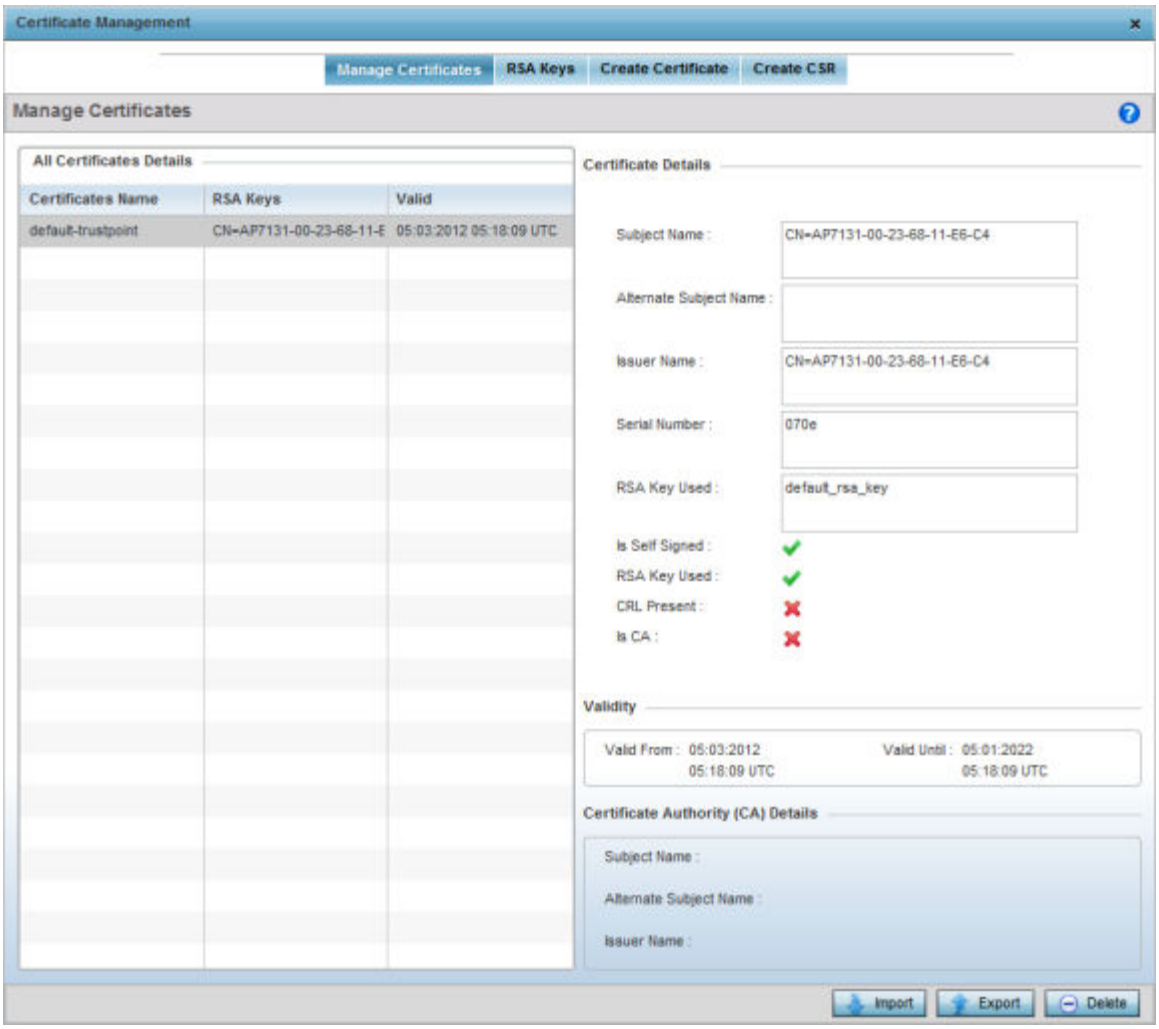



**Figure 131: Certificate Management - Manage Certificates Screen**

2 Select a device from amongst those displayed to review its certificate information.

Refer to Certificate Details field to review the certificate's properties, self-signed credentials, validity period and CA information.

3 To optionally import a certificate, select the **Import** button from the Certificate Management screen. The import trustpoint window displays.

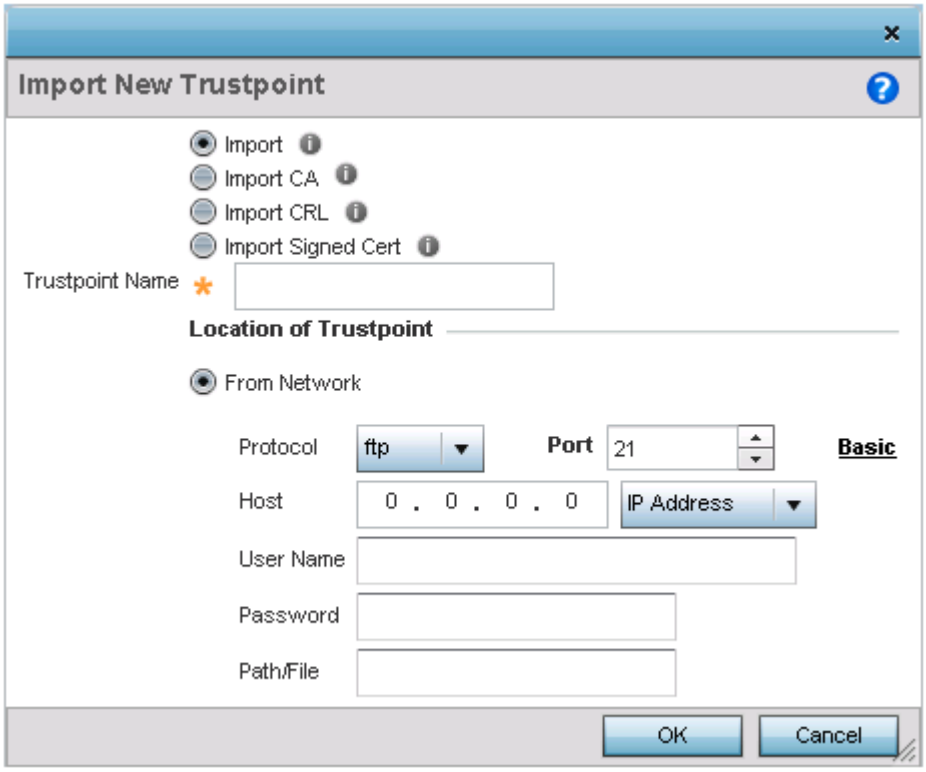



**Figure 132: Import New Trustpoint Window**

4 Define the following configuration parameters required to import the trustpoint:

| | |
|---|---|
| Import | Select the type of Trustpoint to import. The following Trustpoints can be imported:<br>• Import – Select to import any trustpoint.<br>• Import CA – Select to import a Certificate Authority (CA) certificate on to the access point.<br>• Import CRL – Select to import a CRL *(Certificate Revocation List)*, CRLs are used to identify and remove those installed certificates that have been revoked or are no longer valid.<br>• Import Signed Cert – Select to import a self signed certificate. |
| Trustpoint Name | Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. |

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.

If a certificate displays within the Certificate Management screen with a CRL, that CRL can be imported. A CRL *(certificate revocation list)* is a list of revoked certificates, or certificates no longer valid. A certificate can be revoked if the CA improperly issued a certificate, or if a private key is

compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

5 Define the following configuration to import the Trustpoint from a location on the network. To do so, select **From Network** and provide the following information.

| | |
|---|---|
| URL | Provide the complete URL to the location of the trustpoint. This option is available by default. Click the Advanced link next to this field to display more fields to provide detailed trustpoint location information. This option is only available when the **Basic link** is clicked. |
| Protocol | If using Advanced settings, select the protocol used for importing the target trustpoint. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1<br>• usb2<br>• usb3<br>• usb4 |
| Port | If using **Advanced** settings, use the spinner control to set the port. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Host | If using **Advanced** settings, provide the hostname of the server used to import the trustpoint. Select **IPv4 Address** or **IPv6 Address** to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Username/Password | These fields are enabled if using ftp or sftp protocols. Specify the username and the password for that username to access the remote servers using these protocols. |
| Path/File | If using **Advanced** settings, specify the path to the trustpoint. Enter the complete path to the file on the server. |

6 Select the **Cut and Paste** option to paste the trustpoint information in text. When this option is selected, the text box next to it is enabled. Paste the trustpoint details into the text box. This option is only available when *Import CA*, *Import CRL* or *Import Signed Cert* is selected.

7 Select **OK** to import the defined trustpoint.

Select **Cancel** to revert the screen to its last saved configuration.

8 To optionally export a trustpoint to a remote location, select the **Export** button.

Once a certificate has been generated on the authentication server, export the self-signed certificate.

A digital CA certificate is different from a self-signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an Active Directory Group Policy for automatic root-certificate deployment.

Additionally export the key to a redundant RADIUS server so it can be imported without generating a second key. If there are more than one RADIUS authentication servers, export the certificate and do not generate a second key unless you want to deploy two root certificates.

The Export Trustpoint screen displays.

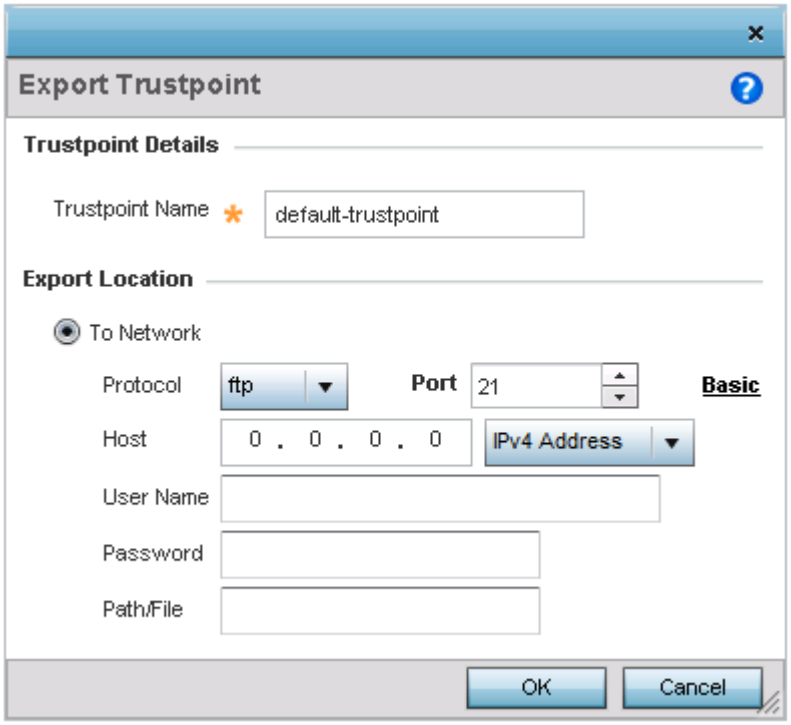



**Figure 133: Export Trustpoint Window**

9 Define the following configuration parameters to export a trustpoint:

| | |
|---|---|
| Trustpoint Name | Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. |
| URL | Provide the complete URL to the location of the trustpoint. If needed, select **Advanced** to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields that populate the screen is dependent on the selected protocol. This option is only available when the **Basic link** is clicked. |

| | |
|---|---|
| Protocol | Select the protocol used for exporting the target trustpoint. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1<br>• usb2<br>• usb3<br>• usb4 |
| Port | If using **Advanced** settings, use the spinner control to set the port. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Host | If using **Advanced** settings, provide the hostname of the server used to export the trustpoint. Select **IPv4 Address** or **IPv6 Address** to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Username/Password | These fields are enabled if using ftp or sftp protocols,. Specify the username and the password for that username to access the remote servers using these protocols. |
| Path/File | If using **Advanced** settings, specify the path to the trustpoint. Enter the complete relative path to the file on the server. |

10 Select **OK** to export the defined trustpoint.

Select **Cancel** to revert the screen to its last saved configuration.

To optionally delete a trustpoint, select the **Delete** button from within the Certificate Management screen. Provide the trustpoint name within the Delete Trustpoint screen and optionally select the **Delete RSA Key** option to remove the RSA key along with the trustpoint. Select **OK** to proceed with the deletion, or **Cancel** to revert to the Certificate Management screen.

*RSA Key Management*

Refer to the RSA Keys screen to review existing RSA key configurations applied to managed devices. If an existing key does not meet the needs of a pending certificate request, generate a new key or import or export an existing key to and from a remote location.

RSA *(Rivest, Shamir, and Adleman)* is an algorithm for public key cryptography. It is an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1 Click the **Launch Manager** button.

The Certificate Management screen displays, with the Manage Certificates tab selected by default. This screen displays all existing trustpoints.

2 Click **RSA Keys**.

The RSA Keys management screen displays.

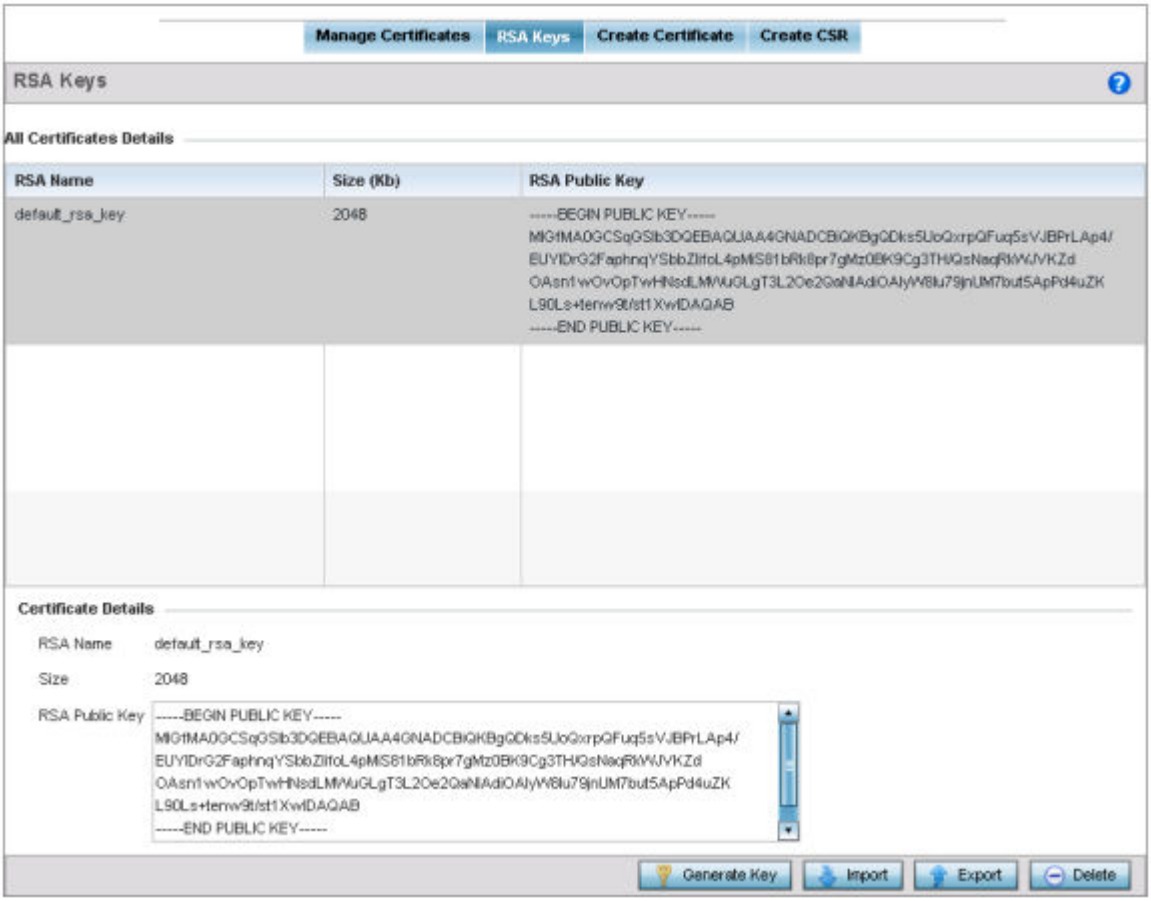



**Figure 134: Certificate Management - RSA Keys Screen**

3 Select a listed device to review its current RSA key configuration.

Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key to a remote location or delete a key from a selected device.

4 Select the **Generate Key** button to create a new key.

The generate RSA key window displays.

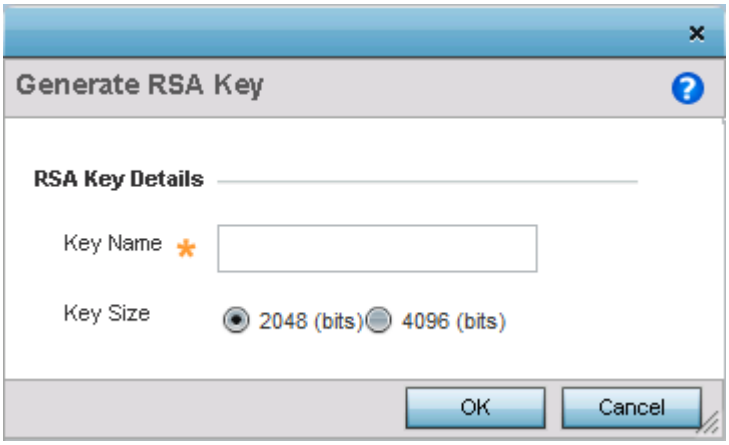



**Figure 135: Generate RSA Key Window**

5 Define the following configuration parameters required to generate a key:

| | |
|---|---|
| Key Name | Enter the 32 character maximum name assigned to the RSA key. |
| Key Size | Use the spinner control to set the size of the key (from 2,048 or 4096 bits). It is recommended leaving this value at the default setting of 2048 to ensure optimum functionality. |

6 Select **OK** to generate the RSA key.

Select **Cancel** to revert the screen to its last saved configuration.

7 To optionally import a CA certificate, select the **Import** button from the RSA Keys screen.

The import RSA Key window displays.

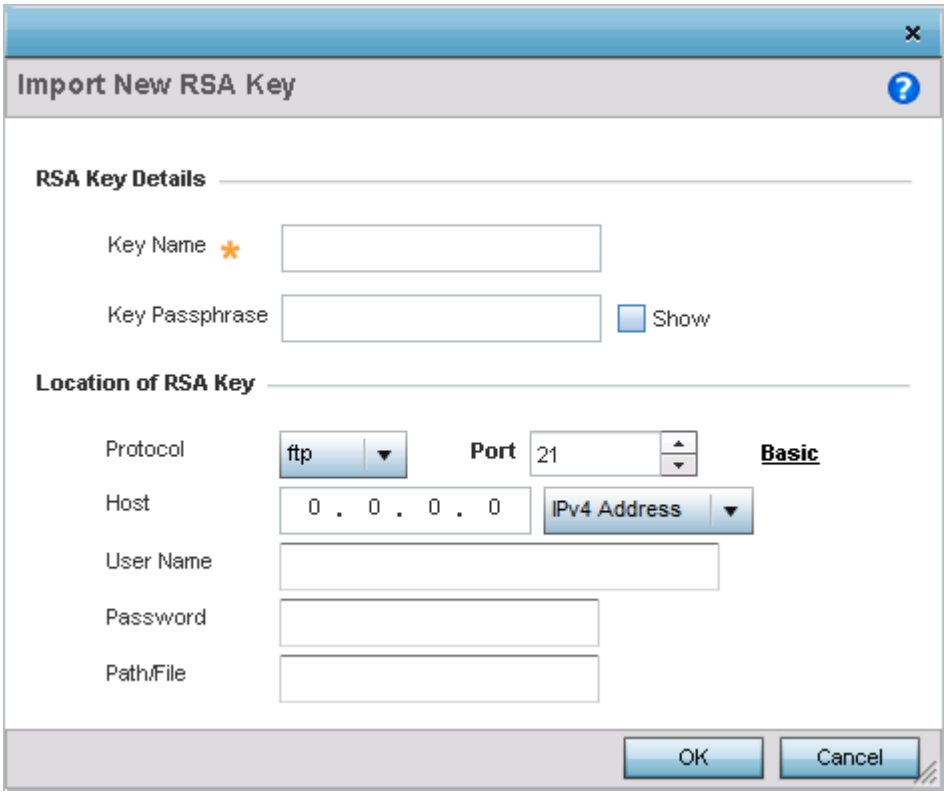



**Figure 136: Import New RSA Key Window**

8 Define the following configuration parameters required to import a RSA key:

| | |
|---|---|
| Key Name | Enter the 32 character maximum name assigned to the RSA key. |
| Key PassPhrase | Define the key used by both the access point and the server (or repository) of the target RSA key. Select the Show option to expose the actual characters used in the passphrase. Leaving the Show option unselected displays the passphrase as a series of asterisks "*". |
| URL | Provide the complete URL to the location of the RSA key. This option is only available when the **Basic link** is clicked. |
| Protocol | If using **Advanced** settings, select the protocol used for importing the target trustpoint. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1<br>• usb2<br>• usb3<br>• usb4 |

| | |
|---|---|
| Port | If selecting Advanced, use the spinner control to set the port. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Host | If selecting **Advanced**, provide the hostname of the server used to import the RSA key. Select **IPv4 Address** or **IPv6 Address** to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Username/Password | These fields are enabled if using ftp or sftp protocols,. Specify the username and the password for that username to access the remote servers using these protocols. |
| Path/File | If selecting **Advanced**, specify the path to the RSA key. Enter the complete relative path to the key on the server. |

9 Select **OK** to import the defined RSA key.

Select **Cancel** to revert the screen to its last saved configuration.

10 To optionally export a RSA key to a remote location, select the **Export** button from the RSA Keys screen.

Export the key to a RADIUS server so it can be imported without generating a second key. If there are more than one RADIUS authentication server, export the certificate and do not generate a second key unless you want to deploy two root certificates.

The export RSA Keys window displays.

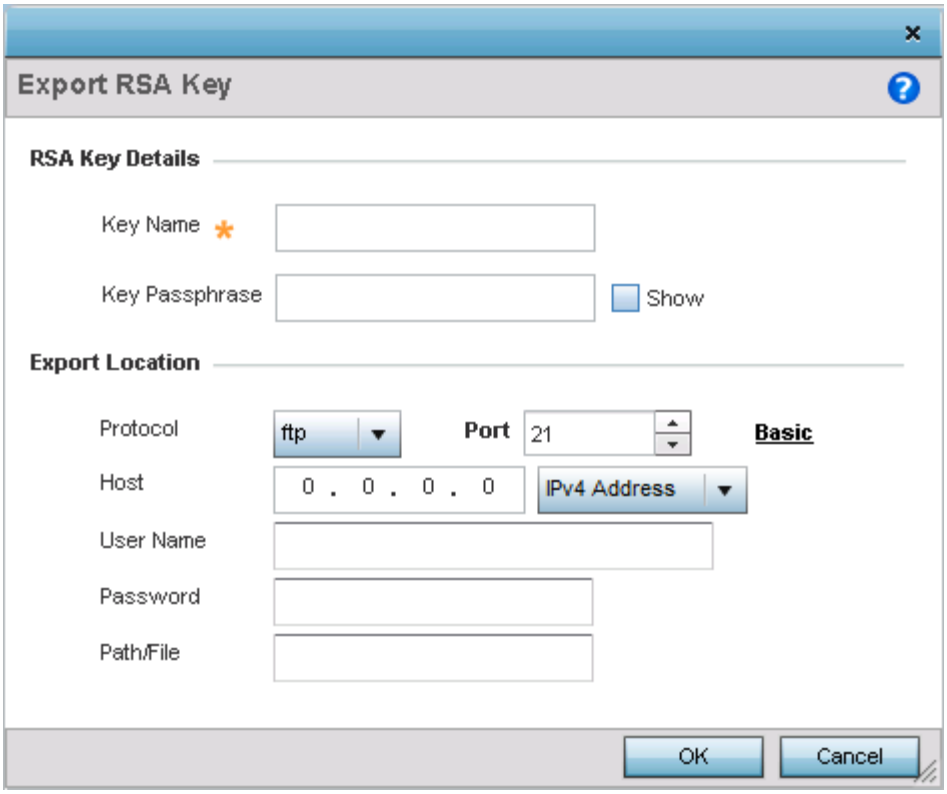



**Figure 137: Export RSA Keys Window**

11 Define the following configuration parameters required to export a RSA key:

| | |
|---|---|
| Key Name | Enter the 32 character maximum name assigned to the RSA key. |
| Key Passphrase | Define the key passphrase used by both the access point and the server. Select the Show option to expose the actual characters used in the passphrase. Leaving the Show option unselected displays the passphrase as a series of asterisks "*". |
| URL | Provide the complete URL to the location of the key. This option is only available when the **Basic link** is clicked. |
| Protocol | If using **Advanced** settings, select the protocol used for importing the target trustpoint. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1<br>• usb2<br>• usb3<br>• usb4 |
| Port | If selecting Advanced, use the spinner control to set the port. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Host | If selecting **Advanced**, provide the hostname of the server used to import the RSA key. Select **IPv4 Address** or **IPv6 Address** to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. |
| Username/Password | These fields are enabled if using ftp or sftp protocols,. Specify the username and the password for that username to access the remote servers using these protocols. |
| Path/File | If selecting **Advanced**, specify the path to the RSA key. Enter the complete relative path to the key on the server. |

12 Select **OK** to export the defined RSA key.

Select **Cancel** to revert the screen to its last saved configuration.

To optionally delete a key, select the **Delete** button from within the RSA Keys screen. Provide the key name within the Delete RSA Key screen and select the **Delete Certificates** option to remove the certificate and the supported key. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

*Certificate Creation*

The Certificate Management screen provides the facility for creating new self-signed certificates. Self-signed certificates (often referred to as root certificates) do not use public or private CAs. A self-signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate:

1 Click the **Launch Manager** button from the SSH RSA Key section.

The Certificate Management screen displays, with the Manage Certificates tab selected by default. This screen displays all existing trustpoints.

2 Select the **Create Certificate** tab.

The Create Certificate screen displays.

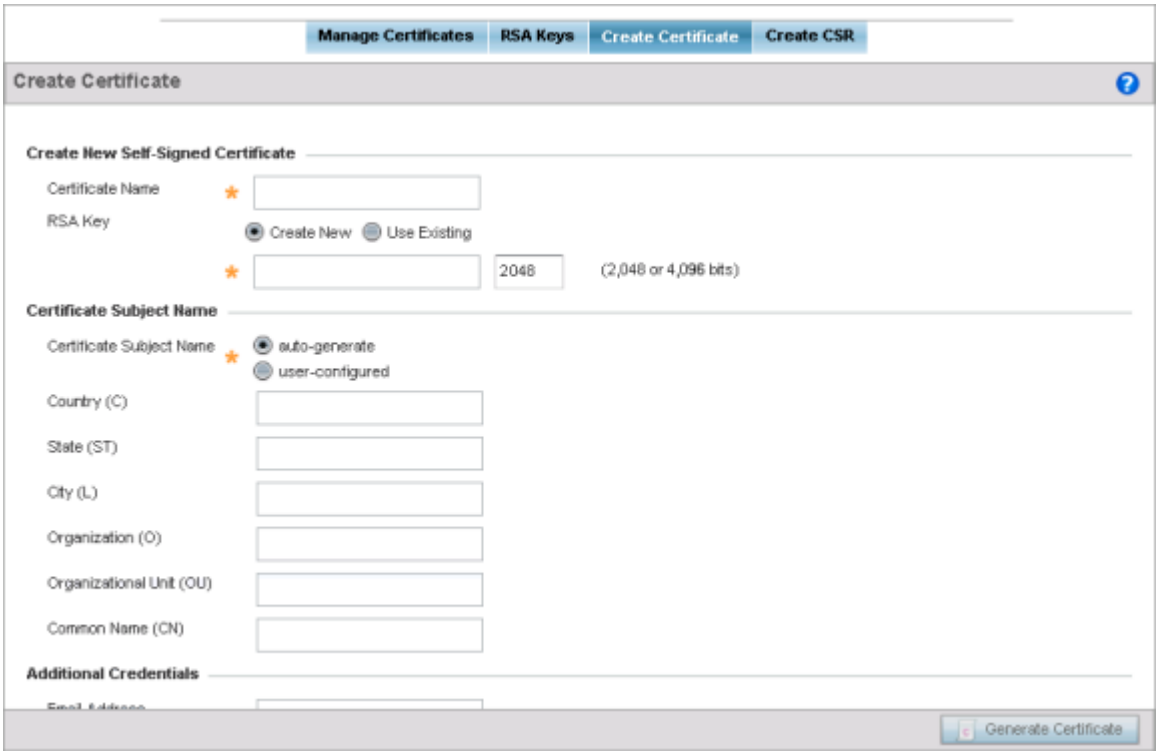



**Figure 138: Create Certificate Window**

3 Set the following Create New Self-Signed Certificate configuration parameters:

| | |
|---|---|
| Certificate Name | Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/ identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate. |
| Use Existing | Select this option to use an existing RSA key. Use the drop-down menu to select the existing key used by both the device and the server (or repository) of the target RSA key. |
| Create New | Select this option to create a new RSA key. Provide a 32 character name to identify the RSA key. Use the spinner control to set the size of the key (from 2,048 or 4,096 bits). It is recommended leaving this value at the default setting (2048) to ensure optimum functionality. For more information on creating a new RSA key, see RSA Key Management on page 308. |

4 Set the following Certificate Subject Name parameters required for the creation of the certificate:

| | |
|---|---|
| Certificate Subject Name | Select either the **auto-generate** radio button to automatically create the certificate's subject credentials or select **user-configured** to manually enter the credentials of the self signed certificate.<br>Note:<br>The default setting is autogenerate. |
| Country (C) | Define the Country of deployment for the certificate. The field can be modified by the user. This is a required field and must not exceed 2 characters. |
| State (ST) | Enter a State for the state or province name used in the certificate. This is a required field. |
| City (L) | Enter a City to represent the city name used in the certificate. This is a required field. |
| Organization (O) | Define an Organization for the organization used in the certificate. This is a required field. |
| Organizational Unit (OU) | Enter an Organizational Unit for the name of the organization unit used in the certificate. This is a required field. |
| Common Name (CN) | If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here. |

5 Set the following Additional Credentials required for the generation of the self-signed certificate:

| | |
|---|---|
| Email Address | Provide an E-mail address used as the contact address for issues relating to this certificate request. |
| Domain Name | Enter a FQDN *(fully qualified domain name)* as an unambiguous domain name that specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. An FQDN differs from a regular domain name by its absoluteness, since s a suffix is not added. |
| IP Address | Specify the IP address used as the destination for certificate requests. |

6 Select the **Generate Certificate** button at the bottom of the screen to generate the certificate.

*Generating a Certificate Signing Request*

A CSR *(certificate signing request)* is an application from a requestor to a certificate authority to issue a digitally signed identity certificate. The CSR is composed of a block of encrypted text generated on the server the certificate will be used on. It contains information included in the certificate, including organization name, common name (domain name), locality and country.

A RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but is used to digitally sign the completed request. The certificate created with a particular CSR only worked with the private key generated with it. If the private key is lost, the certificate is no longer functional. The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1 Select the **Launch Manager** button from the SSH RSA Key section.

The Certificate Management screen displays, with the Manage Certificates tab selected by default. This screen displays all existing trustpoints.

2 Click the **Create CSR** tab.

The Create CSR screen displays.

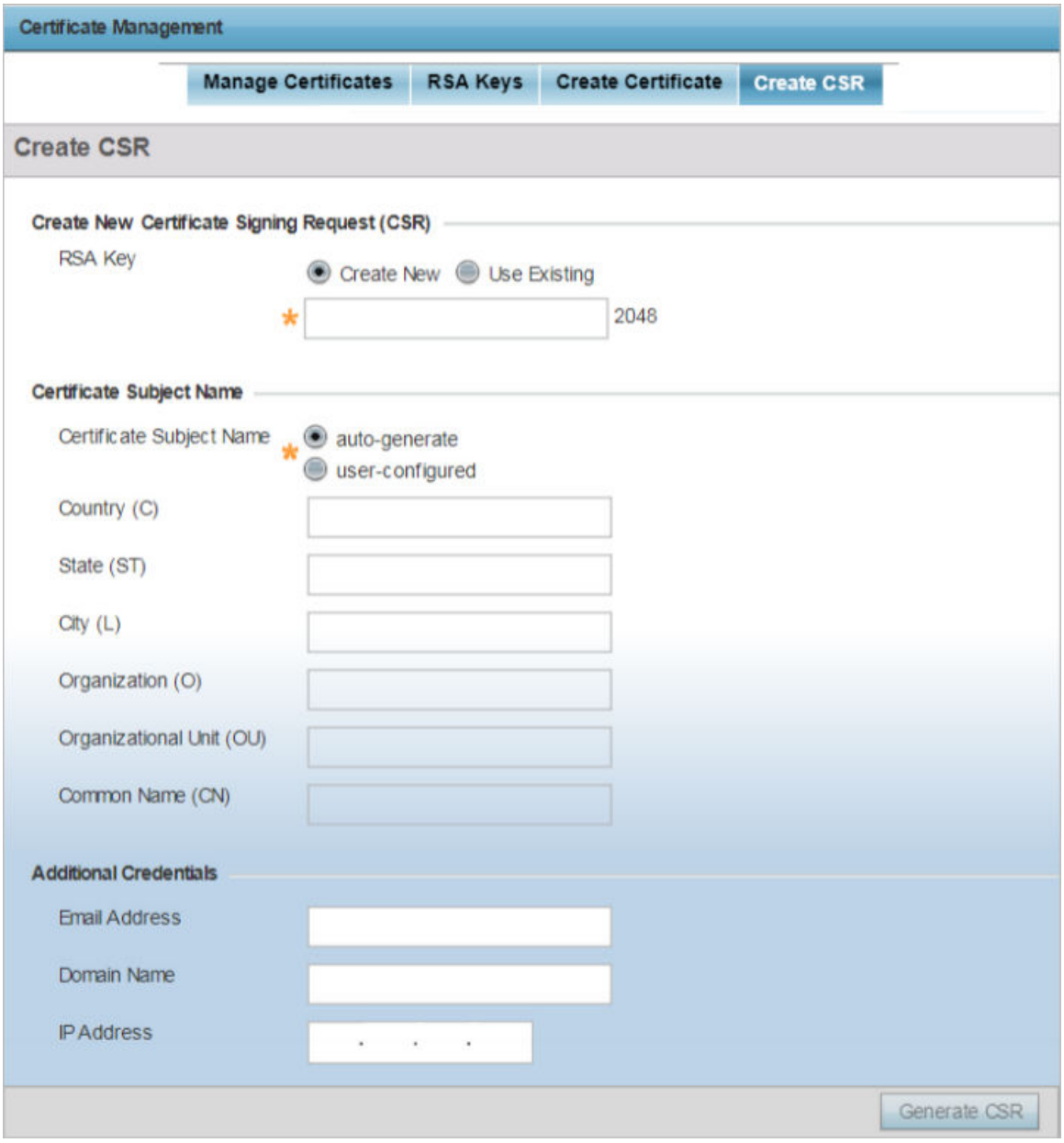



**Figure 139: Create CSR Window**

3 Set the following **Create New Certificate Signing Request (CSR)** configuration parameters:

| | |
|---|---|
| Create New | Select this option to create a new RSA Key. Provide a 32 character name to identify the RSA key. Use the spinner control to set the size of the key (from 2,048 or 4,096 bits). It is recommended leaving this value at the default setting (2048) to ensure optimum functionality. For more information on creating a new RSA key, see RSA Key Management on page 308. |
| Use Existing | Select this option to use an existing RSA key. Use the drop-down menu to select the existing key used by both the device and the server (or repository) of the target RSA key. |

4 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

| | |
|---|---|
| Certificate Subject Name | Select either the auto-generate radio button to automatically create the certificate's subject credentials or select user-configured to manually enter the credentials of the self signed certificate. The default setting is autogenerate. |
| Country (C) | Define the Country used in the CSR. The field can be modified by the user. This is a required field and must not exceed 2 characters. |
| State (ST) | Enter a State for the state or province name used in the CSR. This is a required field. |
| City (L) | Enter a City to represent the city name used in the CSR. This is a required field. |
| Organization (O) | Define an Organization for the organization used in the CSR. This is a required field. |
| Organizational Unit (OU) | Enter an Organizational Unit for the name of the organization unit used in the CSR. This is a required field. |
| Common Name (CN) | If there is a Common Name (IP address) for the organizational unit issuing the certificate, enter it here. |

5 Select the following **Additional Credentials** required for the generation of the CSR:

| | |
|---|---|
| Email Address | Provide an E-mail address used as the contact address for issues relating to this CSR. |
| Domain Name | Enter a FQDN as an unambiguous domain name that specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. An FQDN differs from a regular domain name by its absoluteness, since a suffix is not added. |
| IP Address | Specify the IP address used as the destination for certificate requests. |

6 Select the **Generate CSR** button at the bottom of the Create CSR screen to generate the CSR.

## Wired 802.1x Configuration

802.1X provides administrators secure, identity based access control as another data protection option to utilize with a device profile.

802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the user or device.

To configure the Wired 802.1x settings:

1 Go to **Configuration → Devices → Device Overrides**.

The **Device Overrides** screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays, with the Basic configuration screen selected by default.

3 Select **Wired 802.1x**.

The Wired 802.1X Settings configuration screen displays.

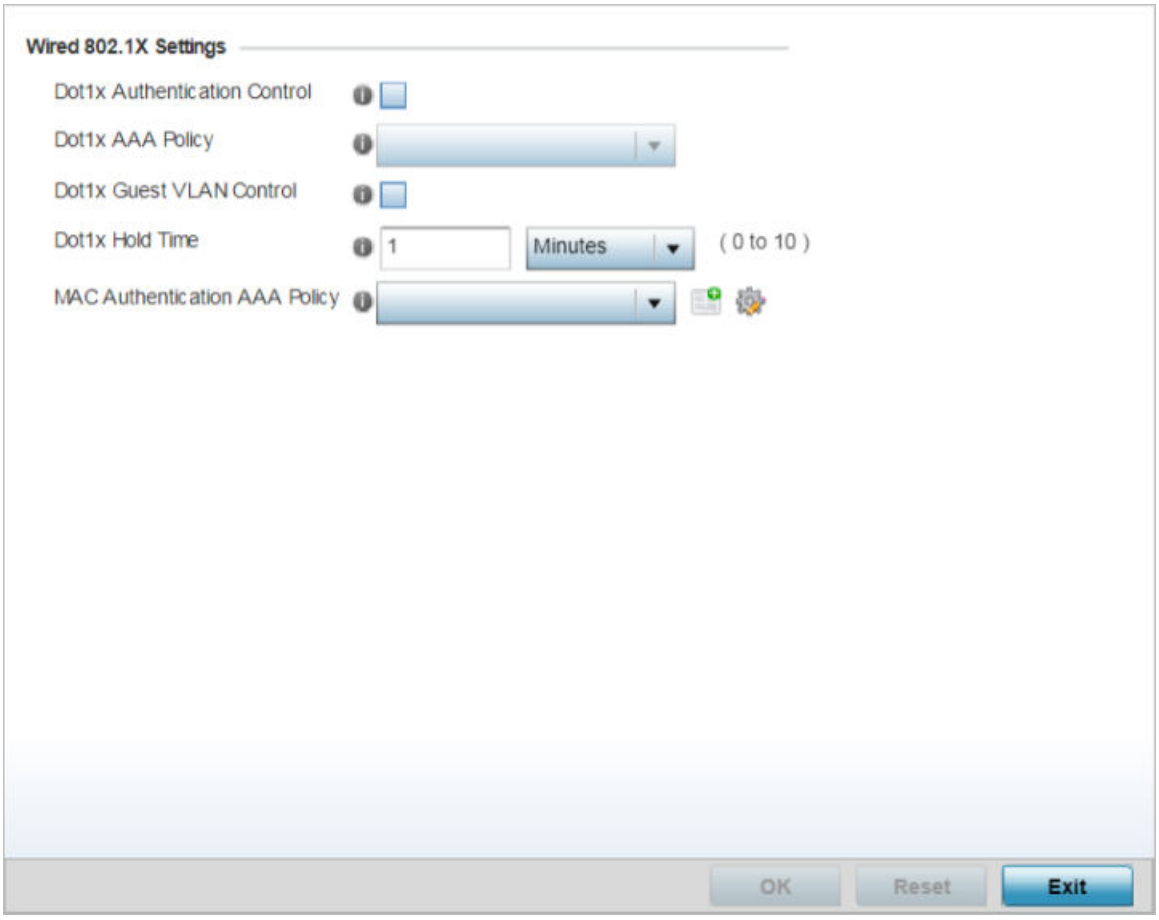



**Figure 140: Device Overrides - Wired 802.1X Settings Screen**

4 Set the following Wired 802.1x Settings:

| | |
|---|---|
| Dot1x Authentication Control | Select this option to globally enable 802.1x authentication for the access point. This setting is disabled by default. |
| Dot1x AAA Policy | Use the drop-down menu to select an AAA policy to associate with the wired 802.1x traffic. If a suitable AAA policy does not exist, click the Create icon to create a new policy or the Edit icon to modify an existing policy. |
| Dot1x Guest VLAN Control | Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default. |

| | |
|---|---|
| Dot1x Hold Time | Set a hold time value (after the last hello packet) in either Seconds (0 - 600) or Minutes (0 - 10). When exceeded, the controller's 802.1X enabled port and its destination end-point connection is defined as lost and the connection must be re-established. |
| MAC Authentication AAA Policy | Use the drop-down menu to select an AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the Create icon to create a new policy or the Edit icon to modify an existing policy. |

5 Select **OK** to save the changes to the 802.1x override configuration.

Select **Reset** to revert to the last saved configuration.

## RF Domain Overrides

Use RF Domain Overrides to define settings overriding a target device's original RF Domain configuration. An RF Domain allows an administrator to assign configuration data to multiple access points (of the same model) deployed in a common coverage area (floor, building or site). In such instances, there are many configuration attributes these devices share as their general client support roles are quite similar. However, device configurations may need periodic refinement from their original RF Domain administered design. Unlike a RFS series controller, an access point supports a single RF domain. An access point RF Domain cannot be used on a different model access point. For example, an AP 6532 RF Domain override can only be applied to another AP 6532 model access point.

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays, with the Basic configuration screen selected by default.

3 Select **RF Domain Overrides**.
The RF Domain configuration overrides screen displays.

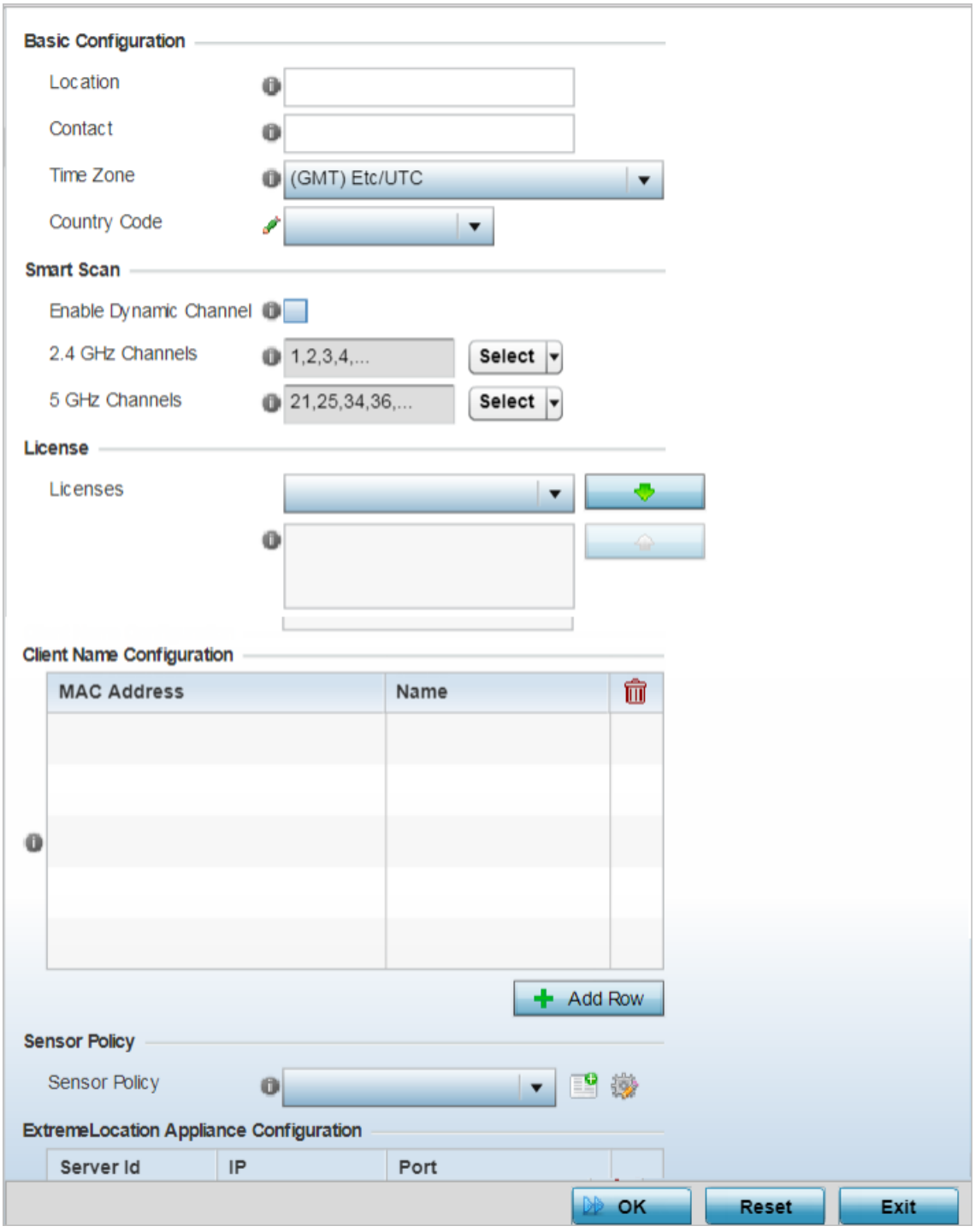



**Figure 141: Access Point - Device Overrides - RF Domain Overrides**

Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove a device's override, go to the *Basic Configuration* screen's *Device Overrides* field, and then select the Clear Overrides button.

4 Refer to the **Basic Configuration** field to review the basic settings defined for the target device's RF Domain configuration, and optionally assign/remove overrides to and from specific parameters.

| | |
|---|---|
| Location | Set the deployment location for the access point as part of its RF Domain configuration |
| Contact | Set the administrative contact for the access point. This should reflect the administrator responsible for the access point's configuration and wireless network. |
| Time Zone | Use the drop-down menu to select the geographic time zone supporting its deployment location |
| Country Code | Use the drop-down menu to select the country code supporting its deployment location |

5 Refer to the **SMART Scan** field to review the settings defined for SMART RF. Optionally assign/remove overrides to and from specific parameters.

| | |
|---|---|
| Enable Dynamic Channel | Select this option to enable dynamic channel scan. |
| 2.4 GHz Channels | Use the **Select** drop-down menu to select channels to scan in the 2.4 GHz band. Selected channels are highlighted with a grey background. Unselected channels are highlighted with a white background. Multiple channels can be selected at the same time |
| 5.0 GHz Channles | Use the **Select** drop-down menu to select channels to scan in the 5.0 GHz band. Selected channels are highlighted with a grey background. Unselected channels are highlighted with a white background. Multiple channels can be selected at the same time |

6 Use the **Licenses** drop-down menu to obtain and leverage feature licenses from RF Domain member devices.

7 Refer to the **Client Name Configuration** table to view the clients connected to RF Domain member access points adopted by networked controllers or service platforms. Use the table to associate administrator assigned client names to specific connected client MAC addresses for improved client management.

Enter the client's factory coded MAC address in the **MAC Address** field. Assign a name to the RF Domain member access point's connected client to assist in its easy recognition in the **Name** field.

8 Use the **Sensor Policy** drop-down menu to either select a sensor policy for sending RSSI information to a dedicated ExtremeLocationing system for device locationing calculations. Different policies can be created with either a default set of scanned channels or with custom channels, widths and weighted scan priorities. Specific channels can also be isolated and locked for specific channel scans.

Note

If a dedicated sensor is utilized with WIPS for rogue detection, any sensor policy selected from the *Sensor Policy* drop-down menu is discarded and not utilized by the sensor. To avoid this situation, use ADSP channel settings exclusively to configure the sensor and not the WiNG interface.

Select the **Create** icon to create a new sensor policy to apply to this RF Domain or select the **Edit** icon to update the configuration of an existing policy before applying it to the RF Domain. For more information, see Sensor Policy on page 671.

9 Within a **ExtremeLocation Appliance Configuration**, sensors scan for RSSI data on an administrator defined interval and send to a dedicated ExtremeLocationing Server resource, as opposed to an

ADSP server. Select the **+ Add Row** button to populate the screen with up to three rows for Locationing server credentials.

| | |
|---|---|
| Server Id | Use the spinner control to assign a numeric ID for up to three ExtremeLocation servers designated to receive RSSI scan data from a WiNG dedicated server. The server with the lowest defined ID is the first reached. The default ID is 1. |
| IP Address/Hostname | Provide the numeric (non DNS) IP address or hostname of up to three ExtremeLocation server resources for receiving RSSI scan data. A hostname cannot exceed 64 characters or contain an underscore. |
| Port | Use the spinner control to specify the port of the ExtremeLocation sensor server resource receiving RSSI scan data from a dedicated sensor. The default port is 443. |

10 In the Tenant Id field, enter the ExtremeLocation tenant's account number. Use this field to configure your ExtremeLocation Tenant account number. ExtremeLocation Tenants, at the time of registration, are communicated (via email) an account number uniquely identifying the Tenant. Configure this account number in the RF Domain context. When configured, RF Domain AP reports, pushed to the ExtremeLocation server, include the Tenant's account number along with the reporting AP's MAC address.

11 Select the Enable NSight Sensor checkbox to enable the NSight module.

12 Click **OK** to save the changes to the sensor configuration.

Click **Reset** to revert to the last saved configuration.

## Device Profile Overrides

A profile enables an administrator to assign a common set of configuration parameters and policies to another access point of the same model. Profiles can be used to assign shared or unique network, wireless and security parameters to access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

However, device profile configurations may need periodic refinement from their original administered design. Consequently, a device profile could require modification from a profile configuration shared amongst numerous devices deployed within a particular site.

Refer to the following to complete the override of the access point's entire profile configuration:


- Profile Overrides - General on page 323
- Profile Overrides - Adoption on page 324
- Profile Overrides - Interface on page 326
- Profile Overrides - Network on page 389
- Profile Overrides - Security on page 464
- Profile Overrides - VRRP on page 496
- Profile Overrides - List of Critical Resources on page 500
- Profile Overrides - Services on page 504
- Profile Overrides - Management Settings on page 507

- Profile Overrides - Meshpoint on page 512
- Profile Overrides - Advanced Client Load Balancing on page 522

*Profile Overrides - General*

To apply overrides to the profile's general configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides**.

The General configuration screen displays by default.

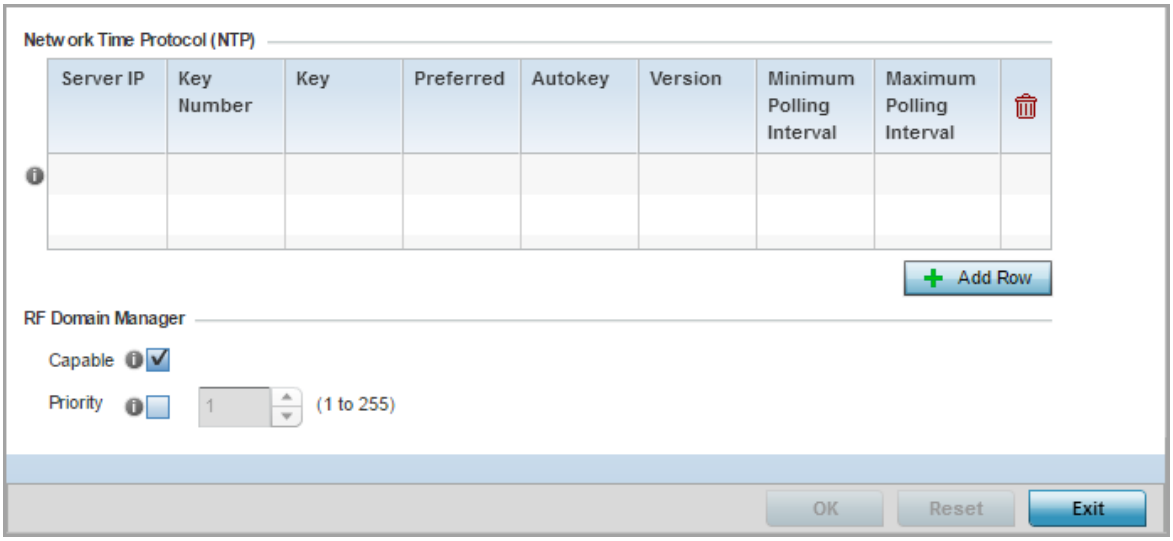



**Figure 142: General Profile Screen**

4 In the Network Time Protocol (NTP) table, click **+ Add Row** and define NTP server resources. These servers are used to obtain system time. Up to three NTP servers can be configured. Set the following parameters to define the NTP configuration:

| | |
|---|---|
| Server IP | Set the IP address of each server added as a potential NTP resource. |
| Key Number | Select the number of the associated authentication peer key for the NTP resource. |
| Key | Enter a 64 character maximum key used when the autokey setting is set to false (disabled). Select the Show option to expose the actual character string comprising the key. |
| Preferred | Select this option to designate this NTP resource as a preferred NTP resource. This setting is disabled by default. |
| AutoKey | Select the check box to enable an autokey configuration for the NTP resource. The default setting is disabled. |
| Version | Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0. |

| | |
|---|---|
| Minimum Polling Interval | Use the drop-down menu to select the minimum polling interval. Once set, the NTP resource is polled no sooner then the defined interval. Options include 64, 128, 256, 512 or 1024 seconds. The default setting is 64 seconds. |
| Maximum Polling Interval | Use the drop-down menu to select the maximum polling interval. Once set, the NTP resource is polled no later then the defined interval. Options include 64, 128, 256, 512 or 1024 seconds. The default setting is 1024 seconds. |

5 Use the RF Domain Manager field to configure how this access point behaves in standalone mode. Set the following parameters:

| | |
|---|---|
| Capable | Select to enable this access point to act as a RF Domain Manager in a particular RF Domain.<br>Note:<br>This option is enabled by default. |
| Priority | Select to prioritize this access point in becoming a RF Domain Manager in its; particular RF Domain. The higher the value, the more likely the device becomes the RF Domain Manager for the domain.<br>Note:<br>This option is disabled by disabled. |

6 Select **OK** to save the general profile configuration changes.

Select **Reset**to revert to the last saved configuration.

*Profile Overrides - Adoption*

To apply overrides to the profile's adoption related configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** and select **Adoption**.

The adoption screen displays. Specify the adoption related overrides to be applied on the selected access point. These changes override the configurations specified on the profile used by the access point..

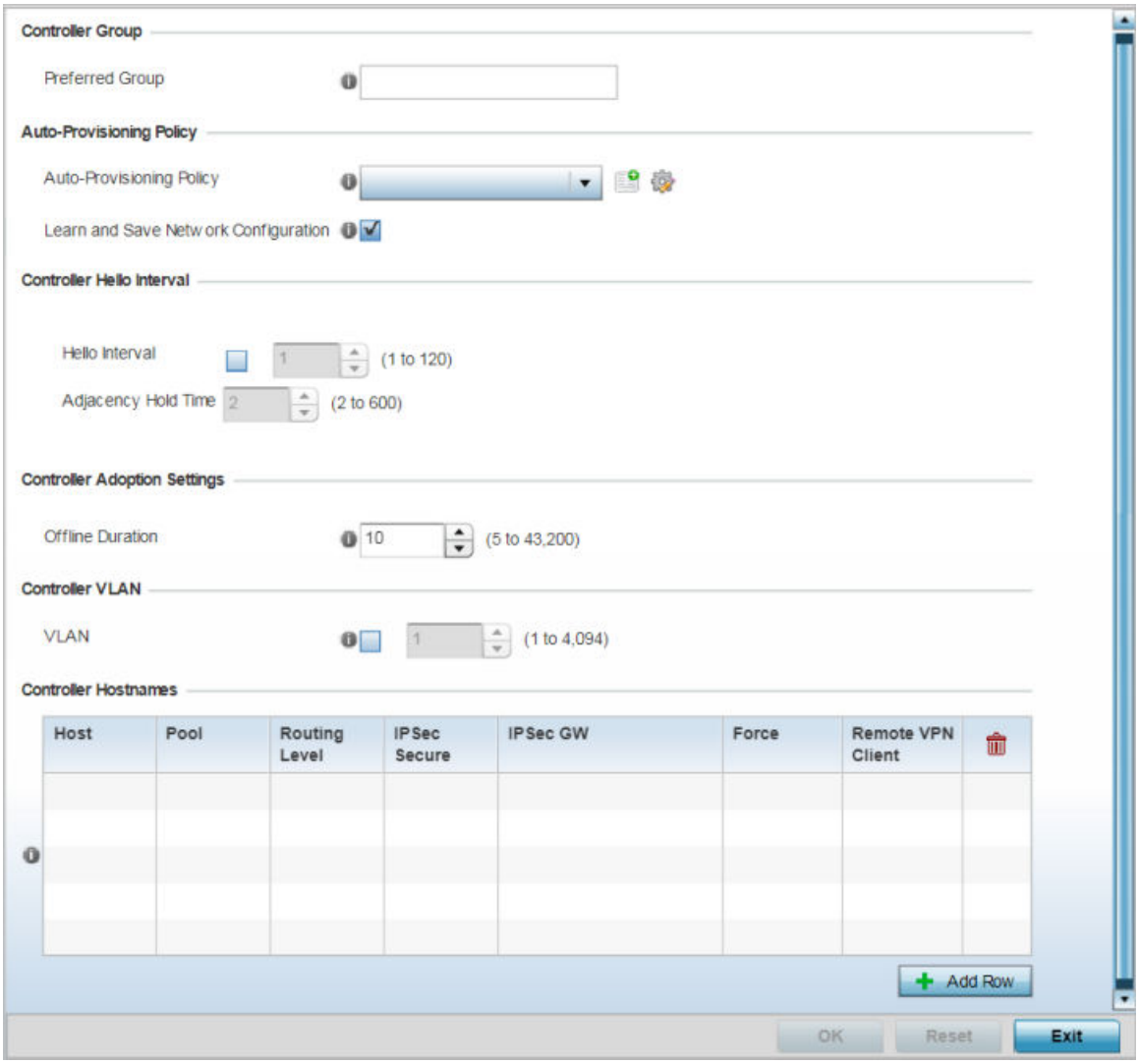



**Figure 143: Profile Overrides - Adoption Screen**

4 Define the **Preferred Group** used as optimal group of controllers for the access point's adoption. The name of the preferred group cannot exceed 64 characters.

The preferred group is the controller group the access point would prefer to connect upon adoption.

5 Set the following Auto-Provisioning Policy settings for access point adoptions:

| | |
|---|---|
| Auto-Provisioning Policy | Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the **Create** icon or modify an existing one by selecting the **Edit** icon. |
| Learn and Save Network Configuration | Select this option to enable allow the controller tor service platform to maintain a local configuration records of devices requesting adoption and provisioning. This feature is enabled by default. |

6 Configure the following Controller Hello Interval settings:

| | |
|---|---|
| Hello Interval | Specify the hello interval in seconds. The hello interval is the interval between two consecutive hello keep alive messages exchanged between the access point and the adopting wireless controller. These messages serve as a connection validation mechanism to ensure the availability of the adopting wireless controller. Use the spinner to set a value from 1 - 120 seconds. |
| Adjacency Hold Time | Specify the adjacency hold time value in seconds. This value sets the time after which the preferred controller group is considered down and unavailable to provide services. Use the spinner to set a value from 2 - 600 seconds.<br>This option is enabled once the hello interval option is selected. |

7 Set the **Offline Duration** time from 5 to 43,200 minutes.

This is the duration for which an adopted access point remains unreachable before being declared as offline by the adopting controller.

8 Select the **VLAN** option to define a VLAN the access point's associating Virtual Controller AP is reachable on. VLANs 0 and 4,095 are reserved and cannot be used. This setting is disabled by default.

9 Enter **Controller Hostnames** as needed to define resources for adoption. Click **+Add Row** to add controllers. Set the following parameters:

| | |
|---|---|
| Allow Adoption of Devices | Select either **`access points`** or **`Controllers`** (or both) to refine whether this controller or service platform can adopt just networked access points or peer controller devices as well. |
| Allow Adoption of this Controller | Select this option to enable this controller or service platform to be capable of adoption by other controllers or service platforms. This setting is disabled by default and must be selected to allow peer adoptions. |
| Preferred Group | If Allow Adoption of this Controller is selected, provide the controller group preferred as the adopting entity for this controller or service platform. If utilizing this feature, ensure the appropriate group is provided within the Controller Group field. |
| Hello Interval | Select this option to define the hello packet exchange interval (from 1 - 120 seconds) between the controller or service platform and an adoption requesting access point. |
| Adjacency Hold Time | Select this option to set a hold time interval (from 2 - 600 seconds) for the transmission of hello packets. |

10 Select **+ Add Row** as needed to populate the table with IP addresses or hostnames of adoption resources.

11 Select **OK** to save the changes made to the general profile configuration. Select **Reset** to revert to the last saved configuration.

### *Profile Overrides - Interface*

An access point requires its Virtual Interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A virtual interface defines which IP address is associated with each connected VLAN ID. An interface configuration can have overrides applied to customize the configuration to a unique deployment objective.

Refer to the following sections:

- Profile Overrides - Ethernet Ports on page 327
- Profile Overrides - Virtual Interface on page 339

- Profile Overrides - Port Channels on page 354
- Profile Overrides - Radios on page 362
- Profile Overrides - PPPoE on page 383
- Profile Overrides - Bluetooth on page 385

### Profile Overrides - Ethernet Ports

To view an access point's ethernet port configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Interface** and select **Ethernet Ports**.

The selected access point's physical port reporting runtime data and statistics is displayed.

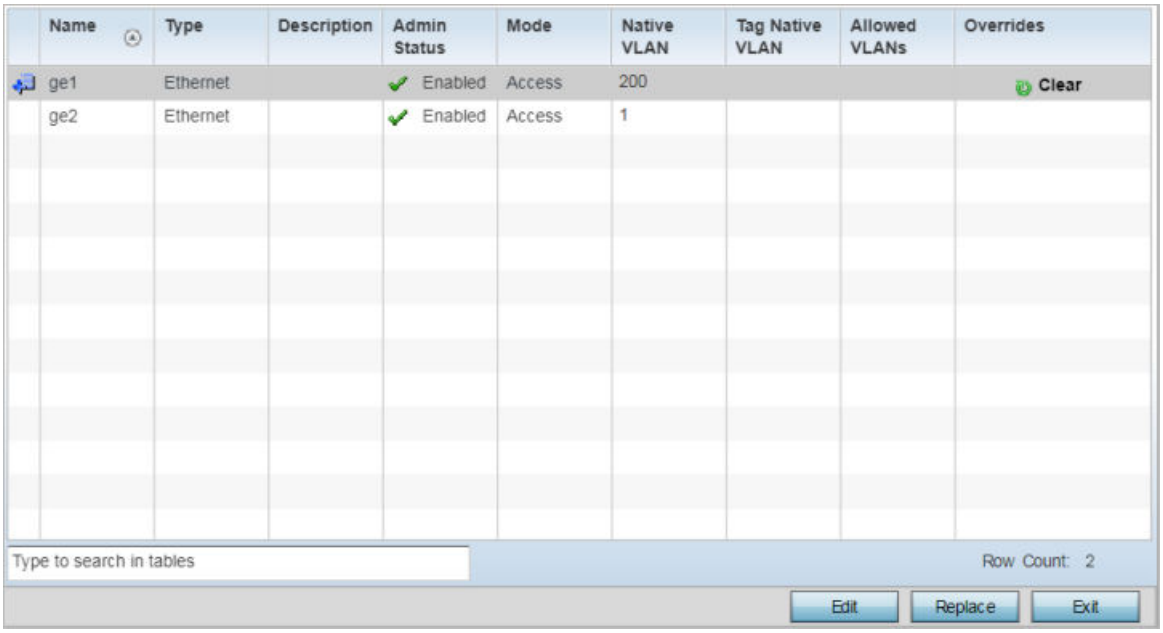



**Figure 144: Profile Overrides - Interface - Ethernet Ports Screen**

4 Refer to the following to assess port status, mode and VLAN configuration:

| | |
|---|---|
| Name | Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on model. |
| Type | Displays the physical port type. |
| Description | Displays an administrator defined description for each listed port. |
| Admin Status | Displays an administrator defined description for each listed port. |

| | |
|---|---|
| Mode | The profile's switching mode: either **Access** or **Trunk** (as defined on the Ethernet Port Basic Configuration screen).<br>If **Access** is selected, the port accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN.<br>If **Trunk** is selected, the port allows packets from a list of VLANs added to the trunk. The port supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged. |
| Native VLAN | The VLAN ID (1 - 4094) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN over which untagged traffic is directed when using a port in **Trunk** mode. |
| Tag Native VLAN | A green check mark means the native VLAN is tagged. A red "X" means the native VLAN is untagged.<br>When a frame is tagged, the 12-bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12-bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. |
| Allowed VLANs | The VLANs allowed to send packets over the listed port. Allowed VLANs are listed only when the port is in **Trunk** mode. |
| Overrides | Select the Clear icon to clear existing overrides applied on the selected device. |

Profile Overrides - Basic Configuration (AP Only)

To edit or apply overrides to an Ethernet port configuration:

1 Select the port and click **Edit**.

The selected Ethernet port's Basic Configuration screen displays by default.

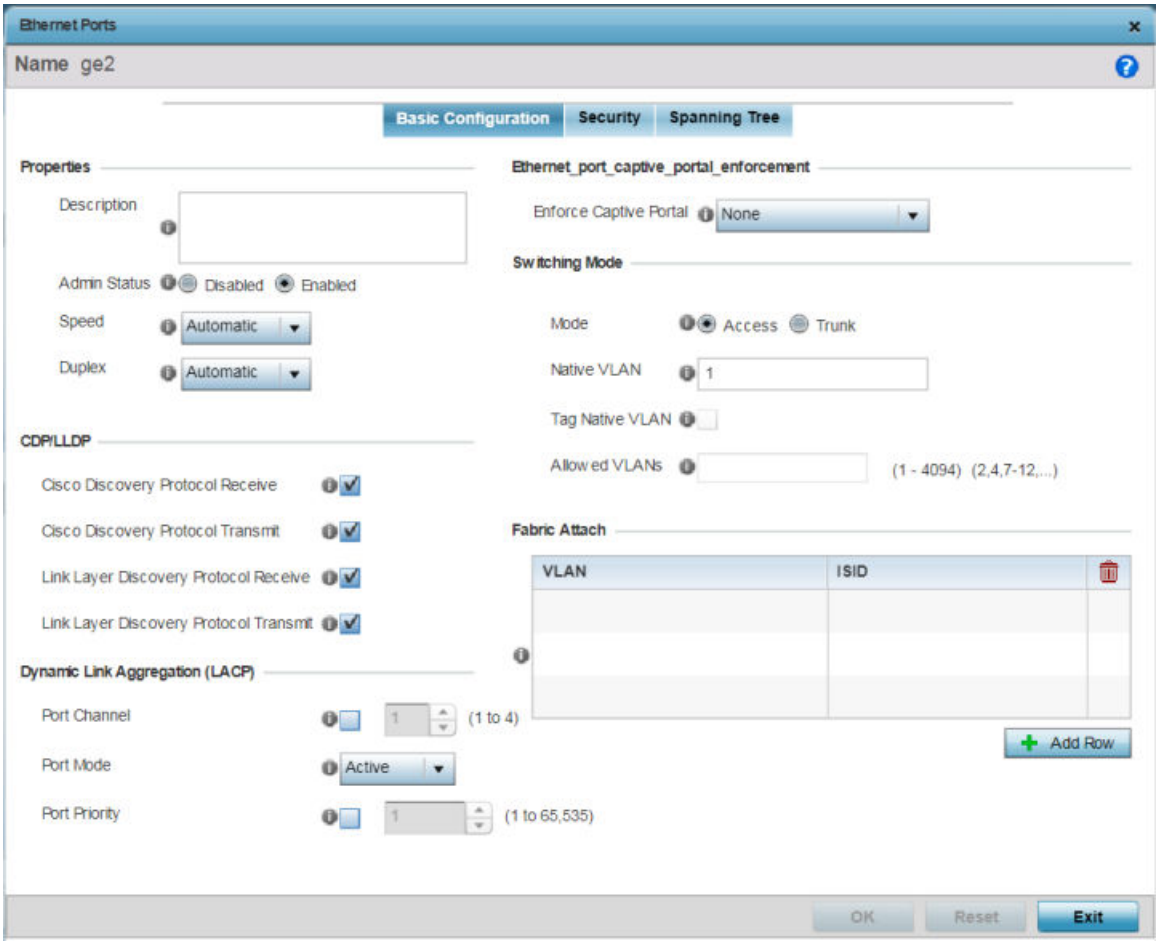



**Figure 145: Profile Overrides - Interface - Ethernet Ports Screen**

2 Set or override the following properties:

| | |
|---|---|
| Description | Enter a brief description for the port (64 characters maximum). The description should reflect the port's intended function to differentiate it from others with similar configurations, or it simply can be the name of the physical port. |
| Admin Status | Select **Enabled** to define this port as active to the profile it supports. Select **Disabled** to disable this physical port in the profile. It can be activated at any time when needed. Admin status is enabled by default. |

| | |
|---|---|
| Speed | Select the speed at which the port can receive and transmit data, to establish a 10, 100, or 1000 Mbps data transfer rate for the selected half-duplex or full-duplex transmission.<br>These options are not available if **`Automatic`** is selected. Select **Automatic** to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis.<br>Automatic is the default setting. |
| Duplex | Select either **`Half`**, **`Full`**, or **`Automatic`** as the duplex option.<br>Select **Half** duplex to send data over the port, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time.<br>Select **Full** duplex to transmit data to and from the port at the same time. Using full duplex, the port can send data while receiving data as well.<br>Select **Automatic** to enable to the controller or service platform to dynamically duplex as port performance needs dictate. **`Automatic`** is the default setting. |

3 Enable or disable the following **CDP/LLDP** parameters used to configure CDP *(Cisco Discovery Protocol)* and LLDP *(Link Layer Discovery Protocol)* for this profile's Ethernet port configuration:

| | |
|---|---|
| Cisco Discovery Protocol Receive | Select this option to allow the Cisco discovery protocol for receiving data on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. |
| Cisco Discovery Protocol Transmit | Select this option to allow the Cisco discovery protocol for transmitting data on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. |
| Link Layer Discovery Protocol Receive | Select this option to allow the Link Layer discovery protocol to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default. |
| Link Layer Discovery Protocol Transmit | Select this option to allow the Link Layer discovery protocol to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. |

4 In the Dynamic Link Aggregation (LACP) area, set the following parameters to enable link aggregation on the selected GE port:

| | |
|---|---|
| Port Channel | Select to configure the selected port as a member of a LAG *(link aggregation group)*. Link aggregation is supported only on the following platforms:<br>LACP enables combining and managing multiple physical connections like Ethernet ports as a single logical channel as defined in the IEEE 802.1ax standard. LACP provides redundancy and increase in throughput for connections between two peers. It also provides automatic recovery in cases where one or more of the physical links - making up the aggregation - fail. Similarly, LACP also provides a theoretical boost in speed compared to an individual physical link.<br><br>Note:<br>if enabling LACP, disable or physically disconnect interfaces that do not use spanning tree to prevent loop formation until LACP is fully configured on both the local and remote devices. |
| Port Mode | Set the port mode as **`Active`** or **`Passive`**. If setting the port as a LAG member, specify whether the port is an active or passive member within the group.<br>An active member initiates and participates in LACP negotiations. It is the active port that always transmits LACPDU irrespective of the remote device's port mode.<br>The passive port only responds to LACPDU received from its corresponding active port.<br>At least one port within a LAG, on either of the two negotiating peers, should be in the active mode. LACP negotiations are not initiated if all LAG member ports are passive. Further, the peer-to-peer LACP negotiations are always initiated by the peer with the lower system-priority value. |
| Port Priority | Select this option and set the selected Ethernet Port's priority value, within the LAG, from 1-65535.<br>The selected port's actual priority within the LAG is determined by the port-priority value specified here along with the port's number. Higher the value, lower is the priority. Use this option to manipulate a port's priority. For example, in a LAG having five physical ports, four active and one standby, manually increasing the standby port's priority ensures that if one of the active port fails, the standby port is included in the LAG during re-negotiation. |

5 Use the Enforce Captive Portal drop-down menu to define whether or not captive-portal authentication is enforced on the selected port:

| | |
|---|---|
| None | Select to prevent captive-portal access permission rules to be enforced. |
| Authentication Failure | Select to apply captive-portal access permission rules only when user authentication fails. |
| Always | Select to enforce captive-portal access permissions at all times. |

6 Override the following Switching Mode parameters:

| | |
|---|---|
| Mode | Set the VLAN switching mode over the port. The options are:<br>**Access** - select to enable the port accept packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. This is the default setting.<br>**Trunk** - select to enable the port allow packets from a list of VLANs you add to the trunk. The port supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged. |
| Native VLAN | Define a VLAN ID (1 - 4094) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN over which untagged traffic is directed when using a port in **Trunk** mode. The default VLAN is 1. |
| Tag Native VLAN | Select this option to tag the native VLAN. Controller and service platforms support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 -bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default. |
| Allowed VLANs | Selecting **Trunk** as the mode enables the **Allowed VLANs** parameter. Add VLANs that exclusively send packets over the listed port. |

7 Click **+ Add Row** and set or override the Fabric Attach parameters. This option enables WiNG devices (access points and controllers) as FA *(Fabric Attach)* clients.

Note

To enable FA Client feature, the Ethernet port's switching mode should be set to trunk.

| | |
|---|---|
| VLAN | Set the VLAN from 1 - 4094. |
| ISID | User the spinner control to specify the ISID from 1 - 16777214. This is the ISID *(Individual Service Identifier)* associated with the VLAN interface specified above.<br>Configuring a VLAN to ISID assignment, enables FA client operation on the selected Ethernet port.<br>The FA Client requests acceptance of the VLAN to ISID mapping from the FAS within the FC *(Fabric Connect)* network. Once acceptance is achieved, the FC edge switch applies the ISID to the VLAN traffic from the device (AP or controller), and uses this ISID inside the Fabric.<br><br>Note:<br>A maximum of 94 pairs of I-SID to VLAN mappings can be configured per Ethernet port. |

FA-enabled switches, in the FC network, send out LLDP messages with TLV extensions of Organization-specific TLV with OUI, to discover FA clients and advertise capabilities.

The FA-enabled client associates with the FAS *(FA Server)*, and obtains provisioning information (management VLAN interface details, and whether the interface is tagged or not) that allows the client to be configured with parameters that allow traffic to flow through the Fabric to the WLAN controller. Use this option to configure the ISID to VLAN mapping that the FA Client uses to negotiate with the FAS.

You can configure FA Client capability on a device's profile as well as device contexts.

8 Click **OK** to save the changes and overrides made to the Ethernet port's Spanning Tree configuration.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Security Configuration (AP Only)

To override Ethernet Ports security settings:

1 Select the **Security** tab.

The security screen displays.

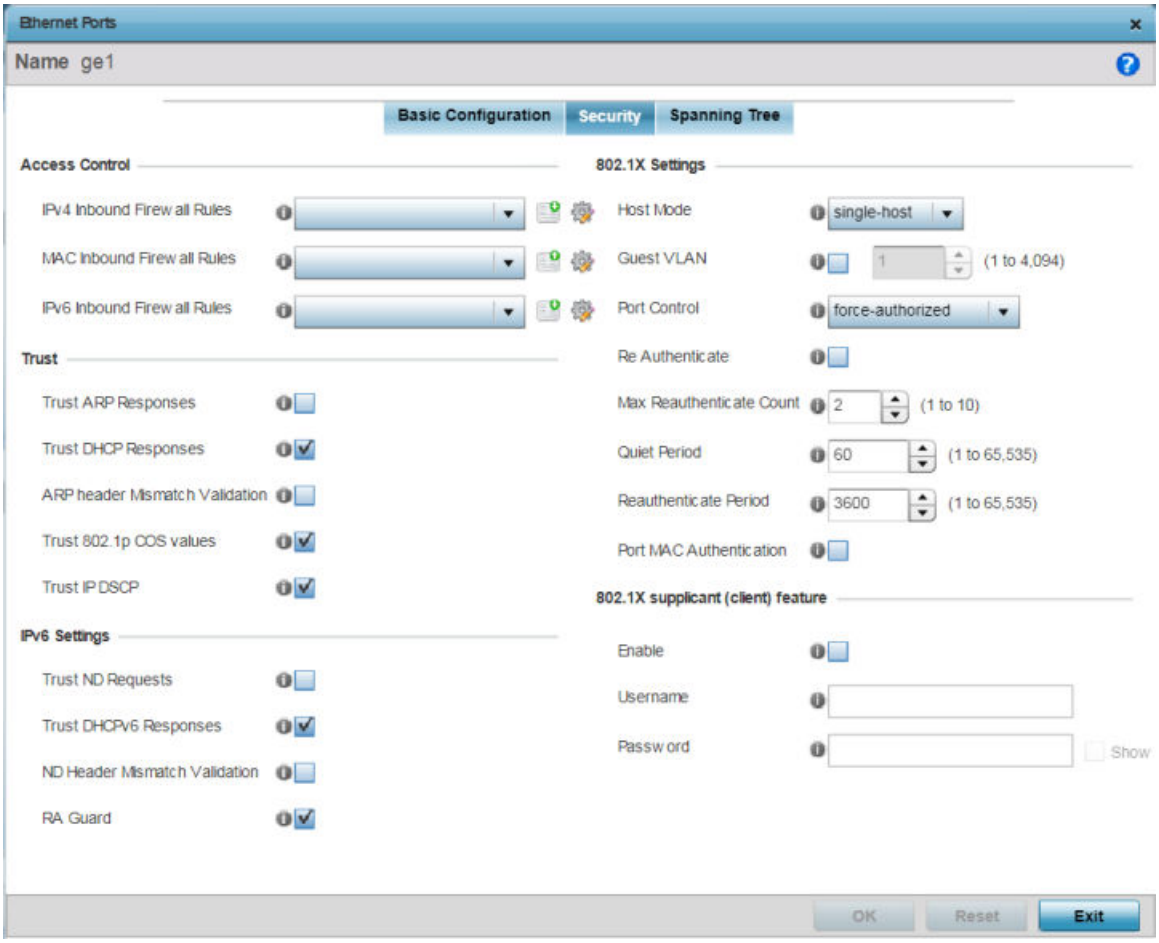



**Figure 146: Profile Overrides - Interface - Ethernet Ports - Security**

2 Refer to the **Access Control** field. As part of the Ethernet port's security configuration, Inbound IP and MAC address firewall rules are required.

| | |
|---|---|
| MAC Inbound Firewall Rules | Use the drop-down menu to select the MAC inbound firewall rules to apply to this profile's Ethernet port configuration. The firewall inspects MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances. |
| IPv4 Inbound Firewall Rules | Use the drop-down menu to select the IPv4 specific firewall rules to apply to this profile's Ethernet port configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity. |
| IPv6 Inbound Firewall Rules | Use the drop-down menu to select the IPv6 specific firewall rules to apply to this profile's Ethernet port configuration. IPv6 is the latest revision of the Internet Protocol designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |

3 Refer to the **Trust** field to define or override the following:

| | |
|---|---|
| Trust ARP Responses | Select this option to enable ARP trust on this port. ARP packets received on this port are considered trusted, and the information from these packets is used to identify rogue devices within the network. This option is disabled by default. |
| Trust DHCP Responses | Select this option to enable DHCP trust on this port. If enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. This option is enabled by default. |
| ARP header Mismatch Validation | Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. This option is disabled by default. |
| Trust 802.1p COS values | Select this option to enable 802.1p COS values on this port. This option is enabled by default. |
| Trust IP DSCP | Select this option to enable IP DSCP values on this port. This option is enabled by default. |

**Note**

Some vendor solutions with VRRP enabled send ARP packets with Ethernet SMAC as a physical MAC and inner ARP SMAC as VRRP MAC. If this configuration is enabled, a packet is allowed, even when a conflict exists.

4 Set the following **IPv6 Settings**:

| | |
|---|---|
| Trust ND Requests | Select this option to enable the trust of neighbor discovery requests required on an IPv6 network on this Ethernet port. This option is disabled by default. |
| Trust DHCPv6 Responses | Select this option to trust all DHCPv6 responses on this Ethernet port. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network. This option is enabled by default. |

| | |
|---|---|
| ND Header Mismatch Validation | Select this option to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This option is disabled by default. |
| RA Guard | Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This option is enabled by default. |

5 Set the following **802.1X Settings**:

| | |
|---|---|
| Host Mode | Set the port mode for 802.1X authentication. The options are:<br>• **single-host** - Select to bridge traffic from a single authenticated host.<br>• multi-host - Select to bridge traffic from any host to this port. The default setting is single-host. |
| Guest VLAN | Specify a guest VLAN for this port from 1 - 4094. This is the VLAN traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled. |
| Port Control | Set the way in which the port bridges traffic. The options are:<br>• **Automatic** – The port is set to the state as received from the authentication server.<br>• **force-authorized** – Any traffic on the port is considered authenticated and is bridged as configured. This the default setting.<br>• **force-unauthorized** – Any traffic on the port is considered unauthenticated and is not bridged. |
| Reauthenticate | Select this option to enable or disable reauthentication. Reauthentication is primarily used to refresh the current state of the selected port. When enabled the device is forced to reauthenticate. When this happens, the port is still considered authenticated. If reauthentication fails, the port is considered unauthorized and devices using the port are denied access. |
| Max Reauthenticate Count | Set the number of reauthentication attempts (1-10) when a port tries to reauthenticate and fails. Once this count exceeds, the port is considered unauthorized. The default setting is 2. |
| Quiet Period | Set the duration in seconds where no attempt is made to reauthenticate a controlled port. Set a value from 0 - 65535 seconds. The default setting is 60 seconds. |
| Reauthenticate Period | Set the duration after which a controlled port is forced to reauthenticate. Set a value from 0 - 65535 seconds. The default setting is 3600 seconds. |
| Port MAC Authentication | Enables MAC address authentication on the selected port. When enabled, a port's MAC address is authenticated, as only one MAC address is supported per wired port. When successfully authenticated, packets from the source are processed. Packets from all other sources are dropped. Port MAC authentication is supported on WiNG devices. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy. This option is disabled by default. |

6 In the 802.1x supplicant (client) feature field, click **Enable** to enable a username and password pair used when authenticating users on this port. Provide the credentials.

Click **Show** to expose the characters in the Password field.

7 Click **OK** to save the changes and overrides made to the Ethernet port's security configuration.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Spanning Tree Configuration (AP Only)

To override the spanning tree configuration:

1 Select the **Spanning Tree** tab.

The selected Ethernet Port's Spanning Tree screen displays.

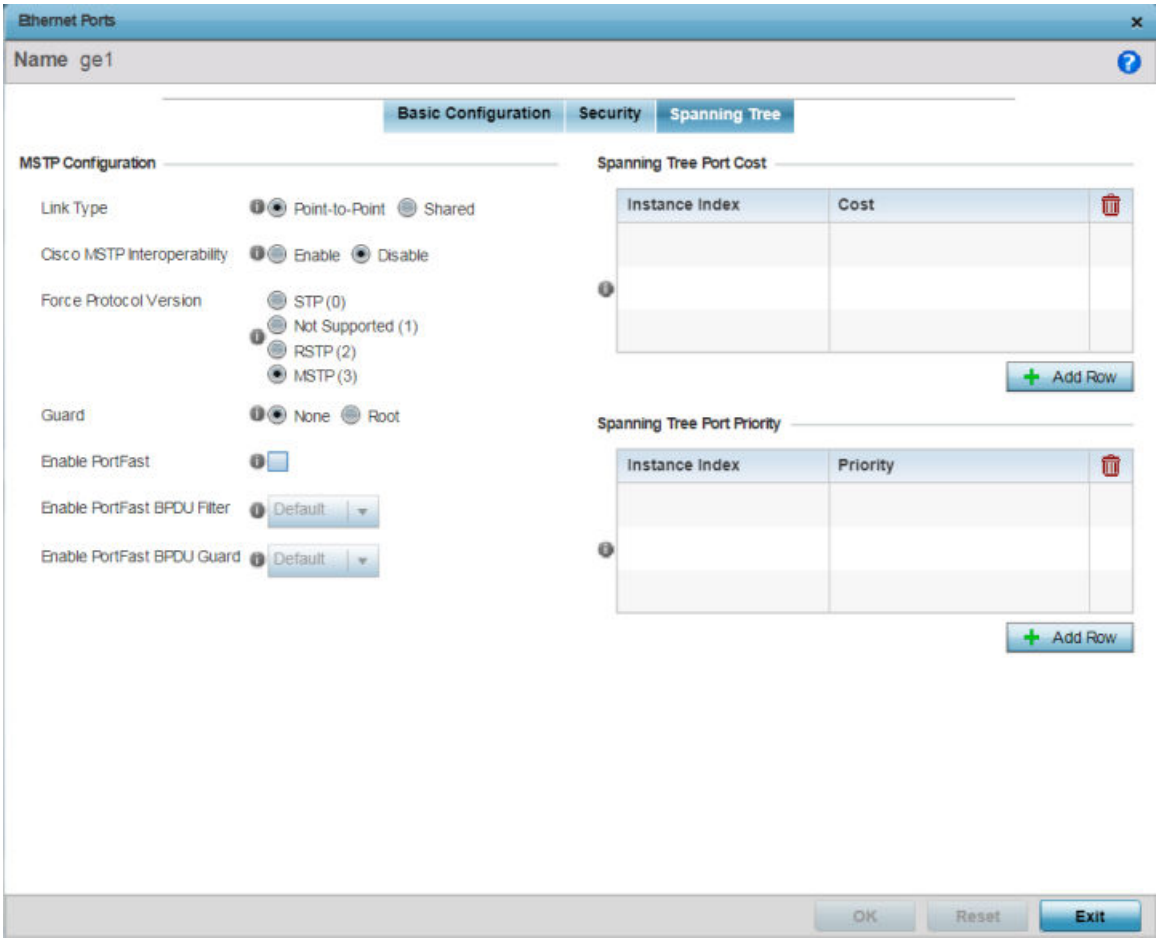



**Figure 147: Profile Overrides - Interface - Ethernet Ports - Spanning Tree**

2 Set the following MSTP Configuration settings:

| | |
|---|---|
| Link Type | Set the link type for this port:<br>• **`Point-to-Point`** - Select to treat the port as connected to a point-to-point link<br>• **`Shared`** - Select to treat the port as shared between multiple devices<br>An example of a *Point-to-Point* connection is a port that is connected to an access point. |
| Cisco MSTP Interoperability | Use to **`Enable`** or **`Disable`** interoperability with Cisco's version of MSTP over the port. Cisco's version of MSTP is incompatible with standard MSTP. |

| | |
|---|---|
| Force Protocol Version | Set the Spanning Tree Protocol to enforce. The options are:<br>• **STP** - Enforces the standard Spanning Tree Protocol.<br><br>STP *(Spanning Tree Protocol)* (IEEE 802.1D standard) configures a meshed network for robustness by eliminating loops within the network and calculating and storing alternate paths to provide fault tolerance.<br><br>As the port comes up and STP calculation takes place, the port is set to **Blocked** state. In this state, no traffic can pass through the port. Since STP calculations take up to a minute to complete, the port is not operational thereby effecting the network behind the port. When the STP calculation is complete, the port's state is changed to **Forwarding** and traffic is allowed.<br>• **RSTP** - Enforces Rapid Spanning Tree Protocol.<br><br>RSTP *(Rapid Spanning Tree Protocol)* (IEEE 802.1w standard) is an evolution over the standard STP. The primary aim is to reduce the time taken to respond to topology changes while being backward compatible with STP. PortFast enables quickly changing the state of a port from Blocked to Forwarding to enable the port to allow traffic while the STP calculation happens.<br>• **MSTP** - Enforces Multiple Spanning Tree Protocol. This is the default setting.<br><br>MSTP *(Multiple Spanning Tree Protocol)* provides an extension to RSTP to optimize the usefulness of VLANs. MSTOP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.<br><br>If there is only one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.<br><br>An MSTP supported deployment uses multiple MST regions with multiple MSTIs *(MST instances)*. Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST). MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP.<br><br>MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI message conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to |

| | |
|---|---|
| | an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.<br>• **`Not Supported`** - Select to disable spanning tree protocol for this interface. |
| Guard | Select **Root** radio to enable root guard – a mechanism to prevent election of roots other than those designated as roots in a network. When this port receives a better (superior) BPDU, the port state becomes Blocked. It retains this state till the port no longer receives the better (superior) BPDU and then the state is changed to Forwarding. Select Root to enable this feature. Select **None** to disable this feature. |

3 Set the following PortFast configuration:

| | |
|---|---|
| Enable PortFast | PortFast reduces the time taken for a port to complete STP. PortFast must only be enabled on ports on the wireless controller which are directly connected to a server/workstation and not to another hub or controller. PortFast can be left unconfigured on the access point.<br>Select this option to enable drop-down menus for both the Enable PortFast BPDU Filter and Enable PortFast BPDU Guard options. This setting is disabled by default. |
| Enable PortFast BPDU Filter | MSTP BPDUs are messages exchanged when controllers gather information about the network topology during STP scan. When enabled, PortFast enabled ports do not transmit or receive BPDU messages. Default sets the PortFast BPDU Filter value to the bridge's BPDU filter value.<br>Select Enable to invoke a BPDU filter for this PortFast enabled port channel. Set Disable to disable this feature. |
| Enable PortFast BPDU Guard | When set to Enable, PortFast enabled ports are forced to shut down when they receive BPDU messages. When set to Default sets the PortFast BPDU Guard value to the bridge's BPDU guard value. Set Disable to disable this feature. |

4 Refer to the Spanning Tree Port Cost table.

Define or override an **Instance Index** using the spinner control, and set its corresponding cost in the Cost column.

This is the cost for a packet to traverse the current network segment. The cost of a path is the sum of all costs of traversal from the source to the destination. The default rule for the cost of a network segment is, the faster the media, the lower the cost.

Select **+ Add Row** as needed to include additional indexes.

5 Refer to the Spanning Tree Port Priority table.

Define or override an **Instance Index** using the spinner control, and set its corresponding priority in the Priority column.

This is the priority for this port becoming a designated root. The default rule is, the lower this value, the higher the chance that the port is assigned as a designated root.

Select **+ Add Row** as needed to include additional indexes.

6 Click **OK** to save the changes and overrides made to the Ethernet port's Spanning Tree configuration.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Virtual Interface

A virtual interface is required for layer 3 (IP) access to a controller or service platform or provide to layer 3 service on a VLAN. The virtual interface defines which IP address is associated with each VLAN ID the controller or service platform is connected to. A virtual interface is created for the default VLAN (VLAN 1) to enable remote administration. A virtual interface is also used to map VLANs to IP address ranges. This mapping determines the destination for routing.

To review an access point's existing VLAN configurations

1 Go to **Configuration → Devices → Device Overrides**.
The Device Overrides screen displays. This screen lists devices within the managed network.
2 Select an access point.
The selected access point's configuration menu displays.
3 Expand **Interface** and select **Virtual Interfaces**.
The existing VLAN configurations are displayed.

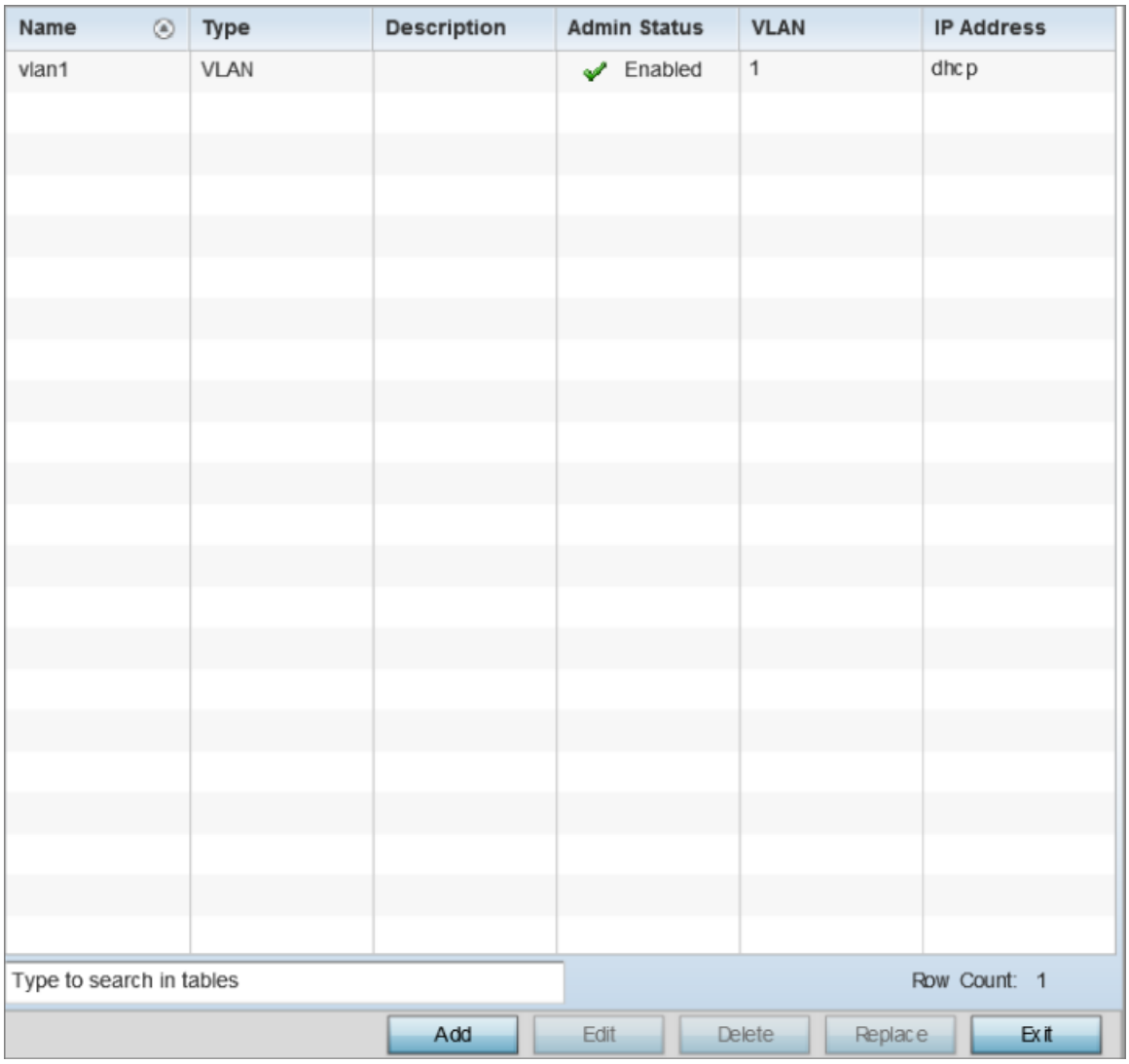



**Figure 148: Profile Overrides - Interfaces - Virtual Interfaces - Main Screen**

4 Review the following parameters unique to each virtual interface configuration:

| | |
|---|---|
| Name | The name of each listed virtual interface assigned when it was created. The name is between 1 - 4094, and cannot be modified as part of a virtual interface edit. |
| Type | The type of virtual interface for each listed interface. |
| Description | The description defined for the virtual interface, either when it was created or when it was edited. |
| Admin Status | A green check mark means the listed virtual interface configuration is active and enabled with its supported profile. A red "X" means the virtual interface is currently shut down. The interface status can be modified when a new virtual interface is created or an existing one modified. |
| VLAN | The numerical VLAN ID associated with each listed interface. |
| IP Address | Whether DHCP was used to obtain the primary IP address used by the virtual interface configuration. |

After reviewing the configurations of existing virtual interfaces, determine whether a new interface needs to be created, an existing virtual interface needs to be edited (overridden), or an existing virtual interface needs to be deleted.

Profile Overrides - Basic - General Configuration (AP Only)

To add a new VLAN configuration or apply overrides to an existing VLAN configuration:

1 Click **Add**, or select the VLAN interface and click **Edit**.

The VLAN interface configuration screen displays, with the **Basic Configuration → General** screen selected by default.

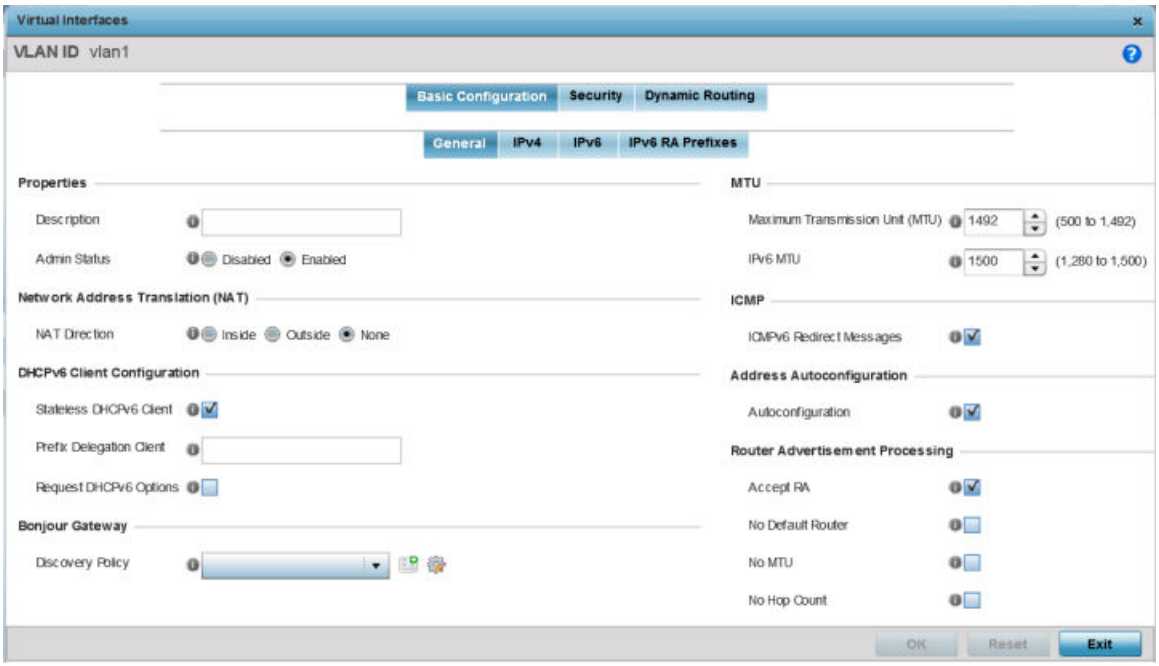



**Figure 149: Profile Overrides - Interfaces - VLAN - Basic Configuration - General Screen**

2 If you are creating a new virtual interface, use the **VLAN ID** spinner control to define a numeric VLAN ID from 1 - 4094.

3 Define or override the following parameters in the Properties field:

| | |
|---|---|
| Description | Provide or edit a description (up to 64 characters) for the virtual interface that helps differentiate it from others with similar configurations. |
| Admin Status | Select **`Disabled`** or **`Enabled`** to define this interface's current status within the network. When set to *Enabled*, the virtual interface is operational and available. The default value is disabled. |

4 Define or override the Network Address Translation (NAT) direction.

Select one of the following options:

| | |
|---|---|
| Inside | Select when the inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. |
| Outside | Select to allow packets passing through the NAT, on the way back to the managed LAN, to be searched against the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the switch managed network. |
| None | Select in case no NAT activity takes place. This is the default setting. |

5 Set the following DHCPv6 Client Configuration.

| | |
|---|---|
| Stateless DHCPv6 Client | Select to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default. |
| Prefix Delegation Client | Specify a 32-character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface. Devices use prefixes to distinguish destinations that reside on-link from those reachable using a router. |
| Request DHCPv6 Options | Select to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than locally. This setting is disabled by default. |

6 In the Bonjour Gateway field, use the Discovery Policy drop-down menu to apply a Bonjour Gateway Discovery policy on the selected VLAN. Click the **Create** icon to define a new Bonjour Gateway policy configuration, or click the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

Bonjour is Apple's implementation of zeroconfiguration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers, and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a LAN *(local area network)*. It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

7 Define the following **MTU** settings for the virtual interface:

| | |
|---|---|
| Maximum Transmission Unit (MTU) | Set the PPPoE client MTU *(maximum transmission unit)* from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492. |
| IPv6 MTU | Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500. |

8 In the **ICMP** field, define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route.

This setting is enabled by default.

9 In the **Address Autoconfiguration** field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits.

This setting is enabled by default.

10 Set the following **Router Advertisement Processing** settings for the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

| | |
|---|---|
| Accept RA | Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters. This setting is enabled by default. |
| No Default Router | Select this option to consider routers unavailable on this interface for default router selection. This setting is disabled by default. |
| No MTU | Select this option to not use the existing MTU setting for router advertisements on this virtual interface. If the value is set to zero, no MTU options are sent. This setting is disabled by default. |
| No Hop Count | Select this option to not use the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default. |

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

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Basic - IPv4 Configuration (AP Only)

To set the selected VLAN interface's IPv4 setting.

1 Select the **Basic Configuration** → **IPv4** tab.

The IPv4 configuration screen displays.

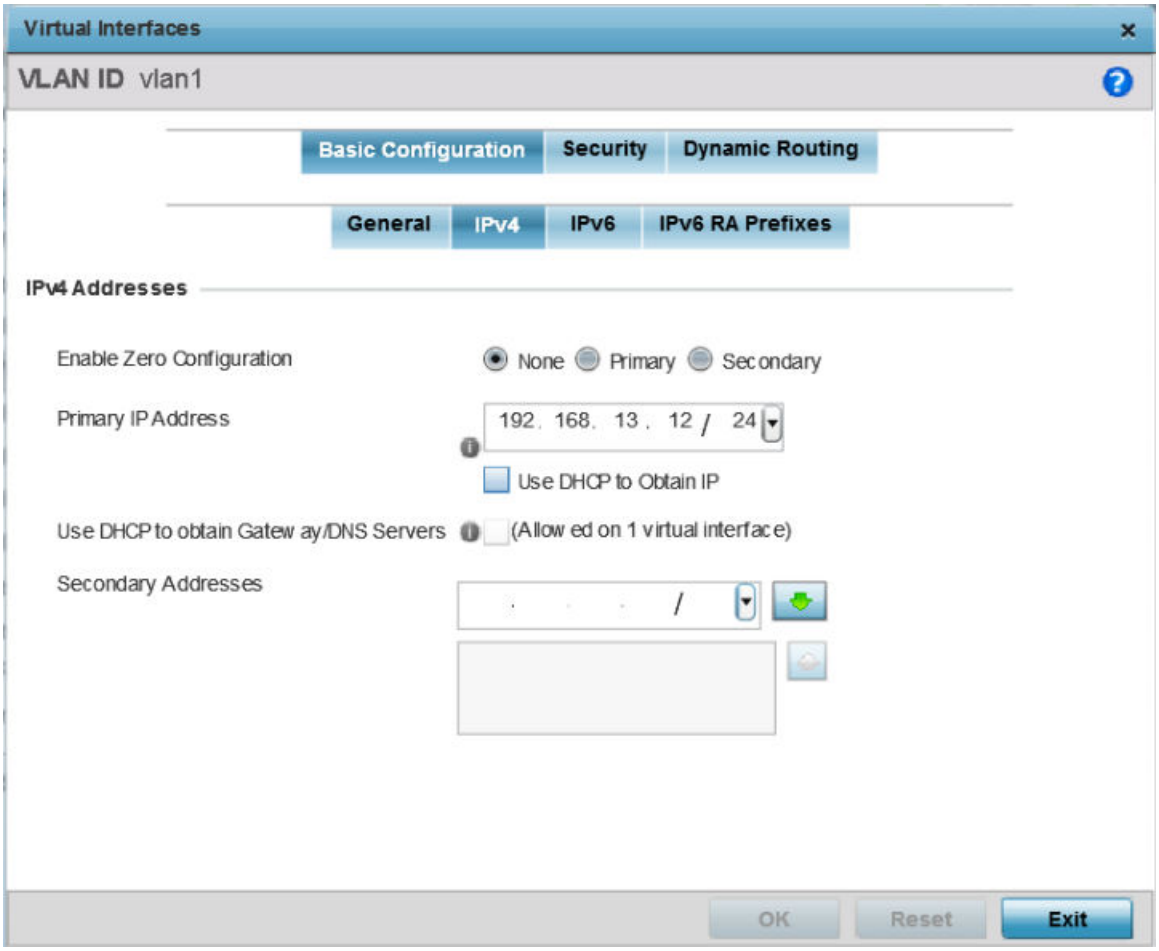



**Figure 150: Profile Overrides - Interfaces - VLAN - Basic Configuration - IPv4 Screen**

2 Set the following network information in the IPv4 Addresses field:

| | |
|---|---|
| Enable Zero Configuration | Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to **None** by default. |
| Primary IP Address | Define the IP address for the VLAN associated virtual interface. |
| Use DHCP to Obtain IP | Select to allow DHCP to provide the IP address for the virtual interface. Selecting this option disables the Primary IP Address field. |

| | |
|---|---|
| Use DHCP to Obtain Gateway/DNS Servers | Select to allow DHCP to obtain a default gateway address and DNS resource for one virtual interface. This setting is disabled by default and only available when the Use DHCP to Obtain IP option is selected. |
| Secondary Addresses | Use this parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable. |

3 Click **OK** to save the changes to the IPv4 configuration.

Click **Exit** to close the screen without saving any updates.

Profile Overrides - Basic - IPv6 Configuration (AP Only)

To set the selected VLAN interface's IPv6 setting.

1 Select the **Basic Configuration** → **IPv6** tab.

The IPv6 configuration screen displays.

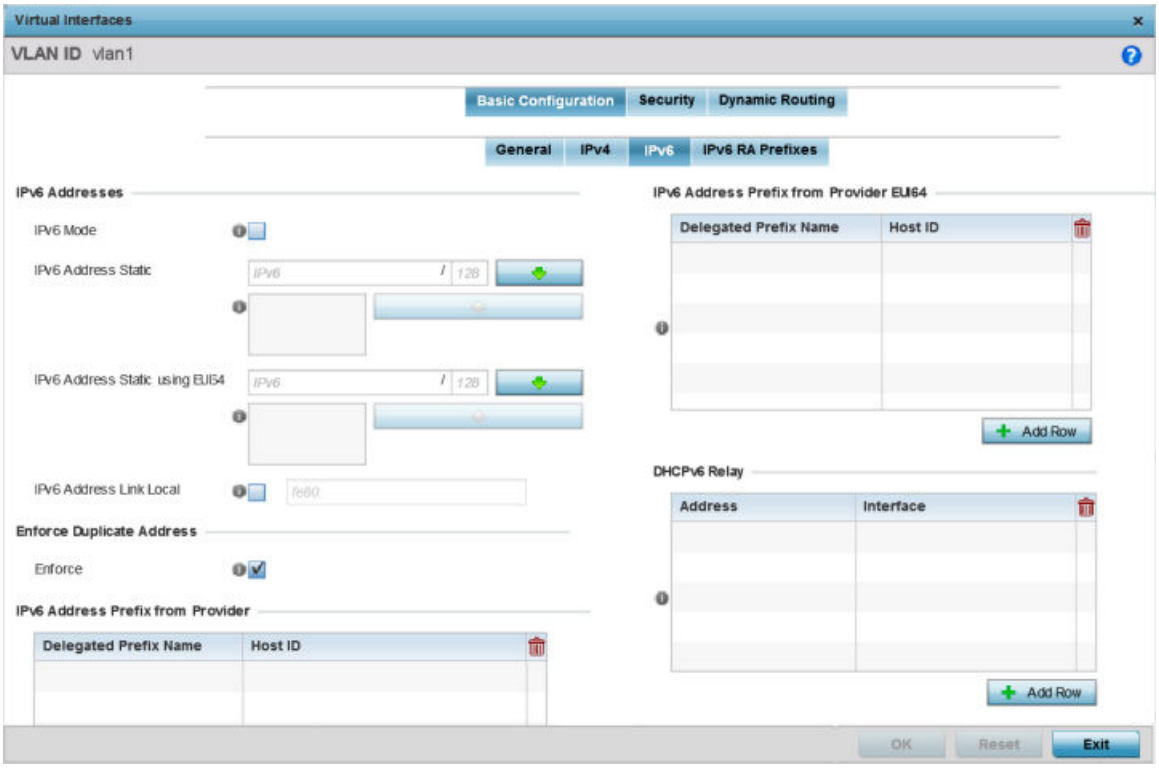



**Figure 151: Profile Overrides - Interfaces - VLAN - Basic Configuration - IPv6 Screen**

2 Refer to the IPv6 Addresses field to define how IP6 addresses are created and utilized:

| | |
|---|---|
| IPv6 Mode | Select this option to enable IPv6 support on this virtual interface. IPv6 is disabled by default. |
| IPv6 Address Static | Define up to 15 global IPv6 IP addresses that can created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons. |

| | |
|---|---|
| IPv6 Address Static using EUI64 | Optionally, set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24- bits, with one being an OUI *(Organizationally Unique Identifier)* and the other being client specific. A 16-bit 0xFFFE is then inserted between the two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address. |
| IPv6 Address Link Local | Provide the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled, even when one or more routable addresses are assigned. |

3 Enable the Enforce Duplicate Address option to enforce duplicate address protection when any wired port is connected and in a forwarding state.

This option is enabled by default.

4 In the IPv6 Address Prefix from Provider table, select **+ Add Row** to create IPv6 format prefix shortcuts as supplied by an ISP.

A new screen is launched. Define the new delegated prefix name and host ID here.

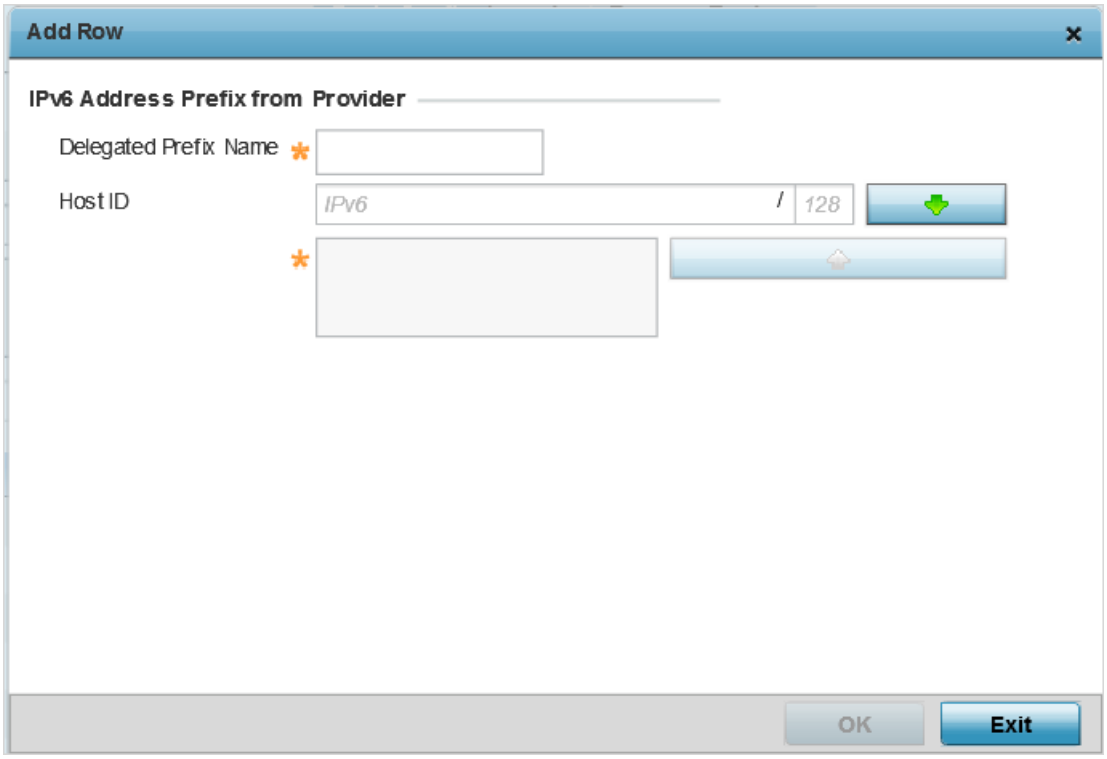



**Figure 152: VLAN Interface - Basic Configuration - IPv6 Screen - IPv6 Address Prefix from Provider Field**

| | |
|---|---|
| Designated Prefix Name | Enter a 32-character maximum name for the IPv6 address prefix from your provider. |
| Host ID | Define the subnet ID, host ID, and prefix length. |

5 Click **OK** to save the changes to the IPv6 configuration.

Click **Exit** to close the screen without saving any updates.

6 In the IPv6 Address Prefix from Provider EUI64 table, click **+ Add Row** to set an (abbreviated) IP address prefix in EUI64 format.

A new screen is launched. Define the new delegated prefix name and host ID can be defined in EUI64 format.

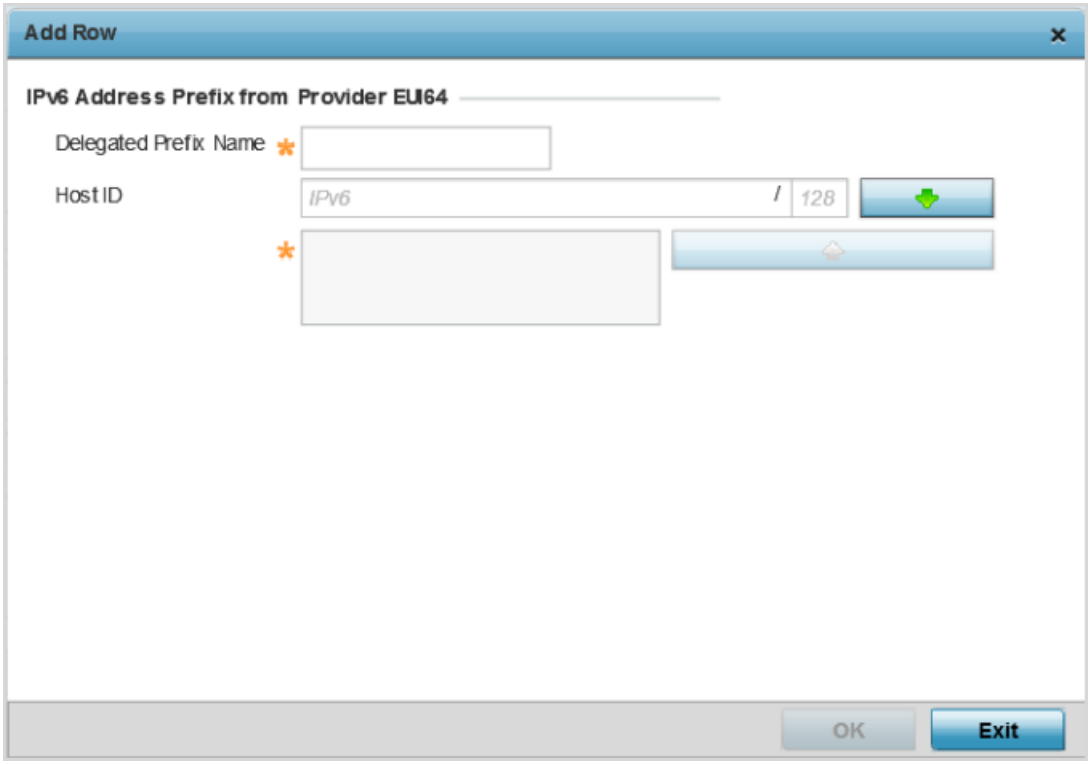



**Figure 153: VLAN Interface - Basic Configuration - IPv6 Screen - IPv6 Address Prefix from Provider EU164 Field**

| | |
|---|---|
| Designated Prefix Name | Enter a 32-character maximum name for the IPv6 prefix from your provider in EUI format. Using EUI64, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without manual configuration or DHCP. |
| Host ID | Define the subnet ID and prefix length. |

7 Click **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format.

Click **Exit** to close the screen without saving any updates.

8 In the DHCPv6 Relay table, select **+Add Row** to set a new DHCPv6 relay address and interface VLAN ID can be set.

A new screen is launched. Define the new DHCPv6 relay address and interface VLAN ID here.

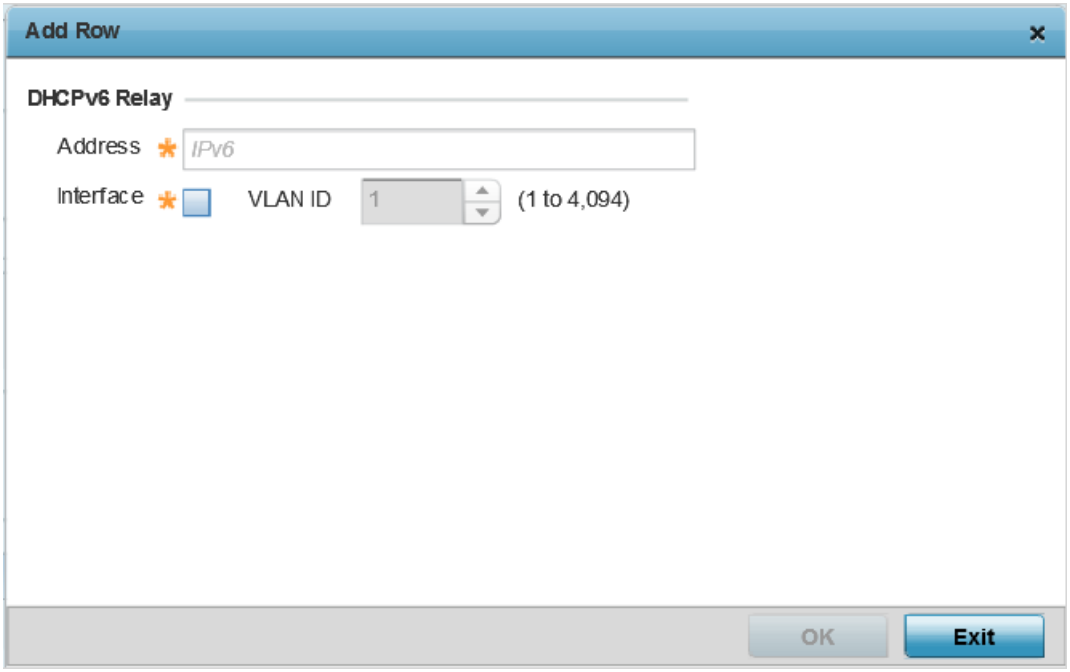



**Figure 154: VLAN Interface - Basic Configuration - IPv6 Screen - DHCPv6 Relay Field**

The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

| | |
|---|---|
| Address | Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network. |
| Interface | Select to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available. |

9 Click **OK** to save the changes to the DHCPv6 relay configuration.

Click **Exit** to close the screen without saving any updates.

Profile Overrides - Basic - IPv6 RA Prefixes Configuration (AP Only)

To set the selected VLAN interface's IPv6 RA Prefixe setting.

1 Select the **Basic Configuration** → **IPv6 RA Prefixes**tab.

The IPv6 RA Prefixes configuration screen displays.

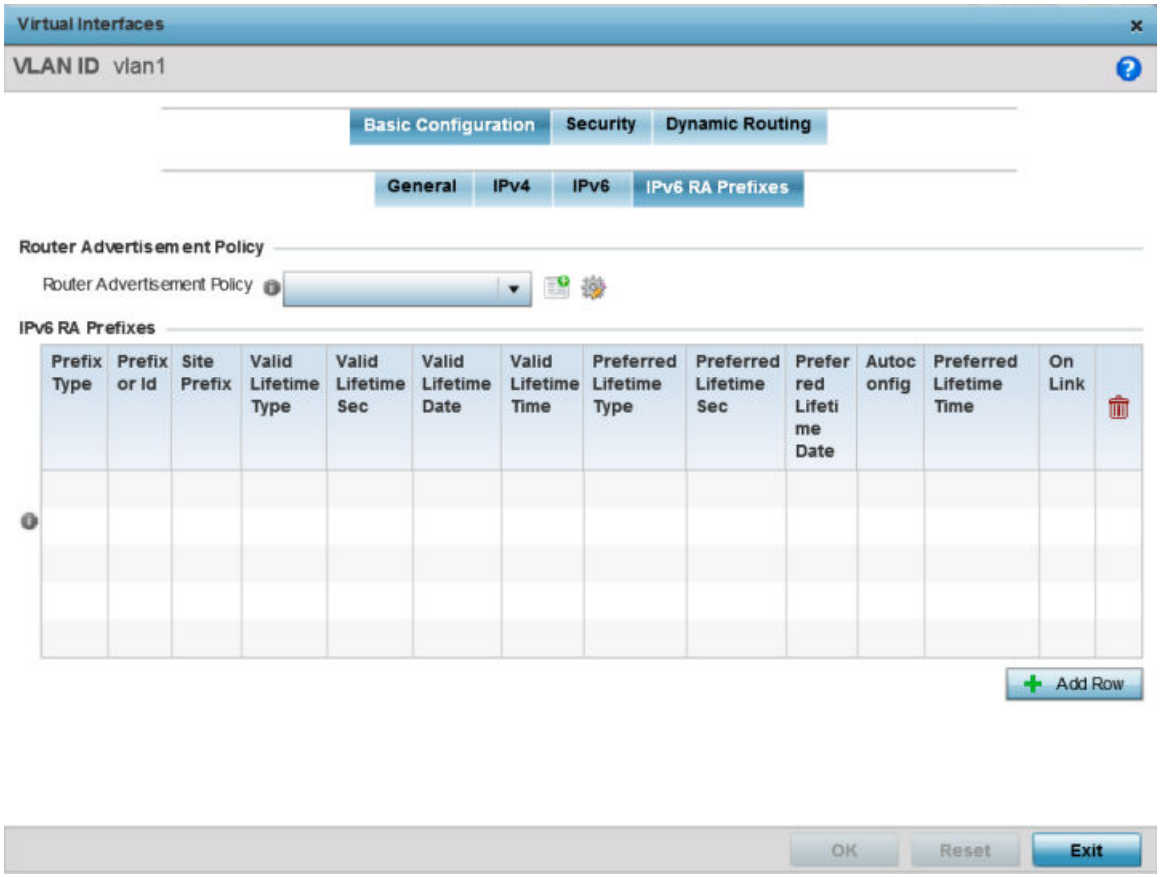



**Figure 155: Profile Overrides - Interfaces - VLAN - Basic Configuration - IPv6 RA Prefixes Screen**

2 Use the Router Advertisement Policy drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

3 Review existing IPv6 advertisement policy configurations. If necessary, select **+ Add Row** to define additional IPv6 RA prefixes.

The add IPv6 RA Prefixes screen displays

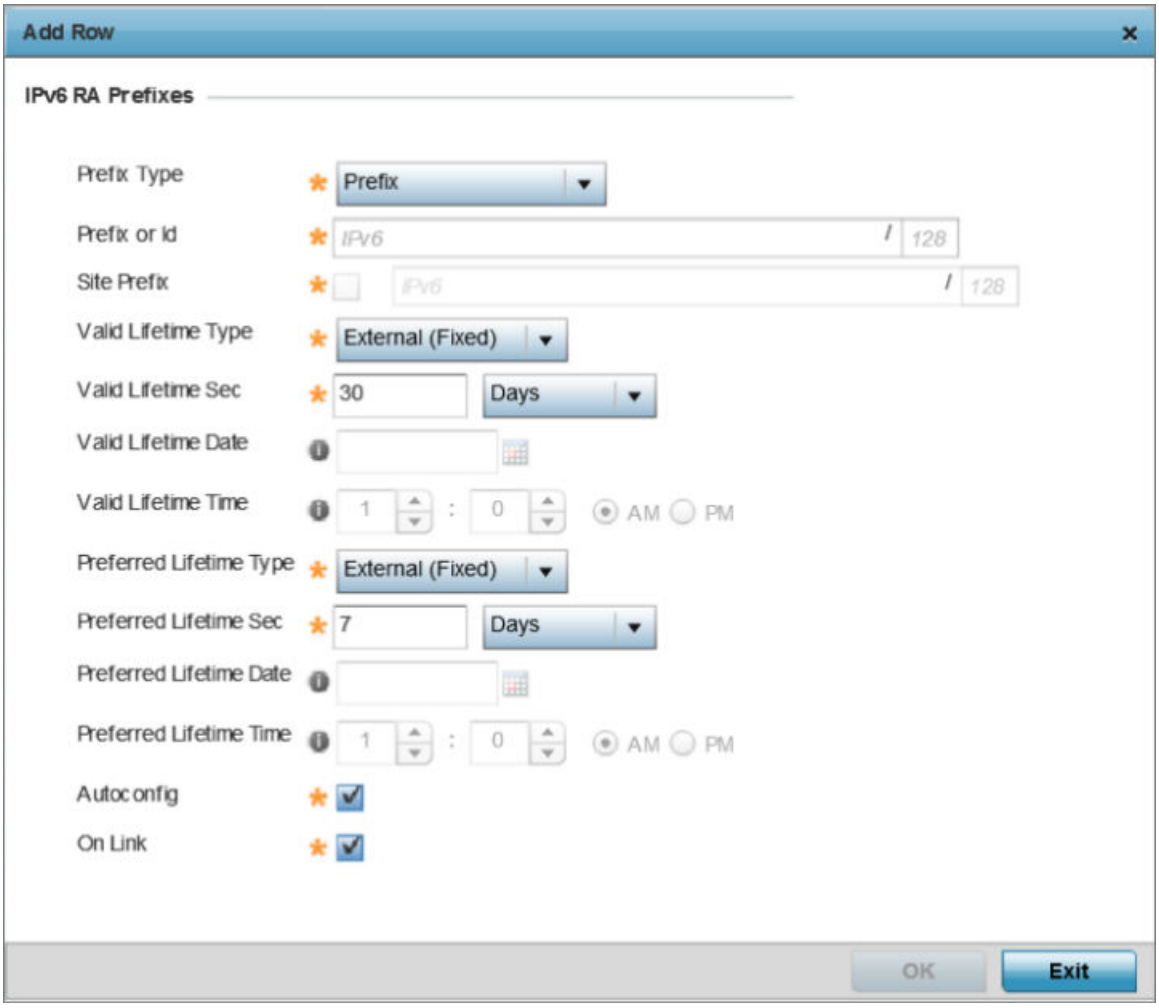



**Figure 156: VLAN Interface - Basic Configuration - Add IPv6 RA Prefixes Screen**

Define the following IPv6 RA Prefix settings:

| | |
|---|---|
| Prefix Type | Set the prefix delegation type used with this configuration. Options include **`Prefix`**, and **`prefix-from-provider`**. The default setting is **`Prefix`**. A prefix allows an administrator to associate a user defined name to an IPv6 prefix. A provider assigned prefix is made available from an ISP *(Internet Service Provider)* to automate the process of providing and informing the prefixes used. |
| Prefix or ID | Set the actual prefix or ID used with the IPv6 router advertisement. |
| Site Prefix | The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link. |
| Valid Lifetime Type | Set the lifetime for the prefix's validity. Options include **`External`** (fixed), **`decrementing,`** and **`infinite`**. If set to **`External`** (fixed), only the **Valid Lifetime Sec** setting is enabled to define the exact time interval for prefix validity. If set to **`decrementing,`**, use the lifetime date and time settings to refine the prefix expiry period. If set to **`infinite`**, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is *External (fixed)*. |

| | |
|---|---|
| Valid Lifetime Sec | If the lifetime type is set to **External** (fixed), set the Seconds, Minutes, Hours, or Days values used to measure the prefix's expiration. 30 days, 0 hours, 0 minutes, and 0 seconds is the default lifetime. |
| Valid Lifetime Date | If the lifetime type is set to **External** (fixed), set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Valid Lifetime Time | If the lifetime type is set to **decrementing**, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the AM and PM radio buttons to set the appropriate hour. |
| Preferred Lifetime Type | Set the administrator preferred lifetime for the prefix's validity. Options include **External** (fixed), **decrementing,** and **infinite**. If set to **External** (fixed), only the **Preferred Lifetime Sec** setting is enabled to define the exact time interval for prefix validity. If set to **decrementing,**, use the lifetime date and time settings to refine the prefix expiry period. If set to **infinite**, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is *External (fixed)*. |
| Preferred Lifetime Sec | If the administrator preferred lifetime type is set to **External** (fixed), set the Seconds, Minutes, Hours, or Days values used to measure the prefix's expiration. 30 days, 0 hours, 0 minutes, and 0 seconds is the default lifetime. |
| Preferred Lifetime Date | If the administrator preferred lifetime type is set to **External** (fixed), set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Preferred Lifetime Time | If the administrator preferred lifetime type is set to **decrementing**, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the AM and PM radio buttons to set the appropriate hour. |
| Autoconfig | Autoconfiguration includes generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default. |
| On Link | Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled. |

4 Click **OK** to save the changes to the IPv6 RA prefix configuration.

Click **Reset** to revert to the last saved configuration. Or, click **Exit** to close the screen without saving any updates.

Profile Overrides - Security Configuration (AP Only)

To define new security settings or apply overrides to existing settings on a VLAN interface:

1 Select the **Security** tab.

The VLAN interface security screen displays.

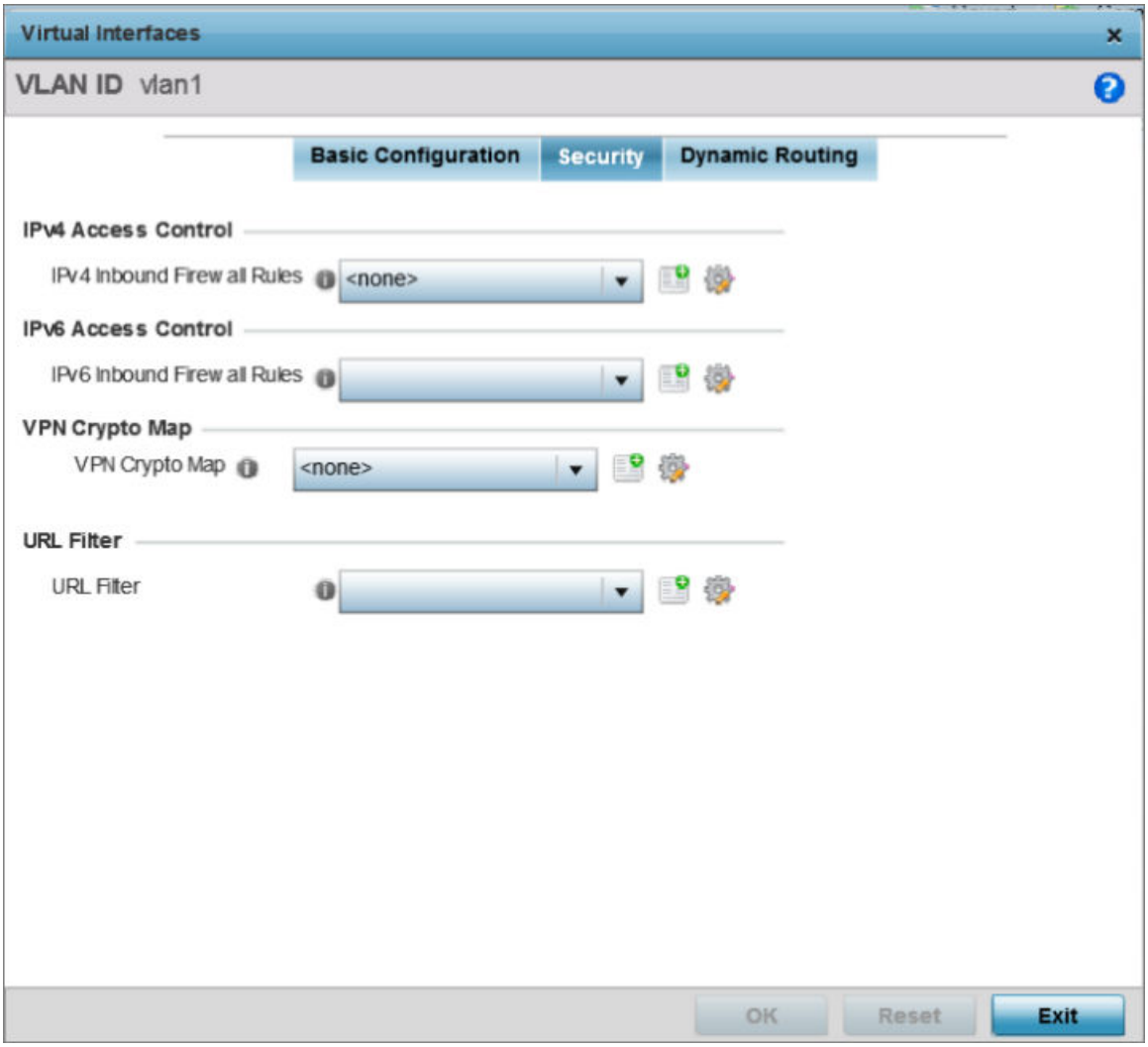



**Figure 157: Profile Overrides - Interface - VLAN Interface - Security Screen**

2 Review the exisiting firewalls applied on the selected VLAN interface. If needed add new firewalls or modfiy existing security settings.

3 Use the IPv4 Inbound Firewall Rules drop-down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration.

Click the **Create** icon to define a new IPv4 firewall rule configuration, or click the **Edit** icon to modify an existing configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, since it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). For more information on creating IPv4 firewall rules, see Setting an IPv4 or IPv6 Firewall Policy on page 745.

IPv4 and IPv6 are different enough to warrant separate protocols. IPv6 devices can alternatively use stateless address autoconfiguration. IPv4 hosts can use link local addressing to provide local connectivity.

4 Use the IPv6 Inbound Firewall Rules drop-down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration.

Click the **Create** icon to define a new IPv6 firewall rule configuration, or click the **Edit** icon to modify an existing configuration.

IPv6 is the latest revision of the Internet Protocol (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. For more information on creating IPv6 firewall rules, see Setting an IPv4 or IPv6 Firewall Policy on page 745.

5 Use the VPN Crypto Map drop-down menu to select or override the Crypto Map configuration applied to this virtual interface.

The VPN Crypto Map entry defines the type of VPN connection and its parameters. For more information see Defining Profile VPN Settings on page 217.

6 Use the URL Filter drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface.

URL filtering is used to restrict access to undesirable resources on the internet.

7 Click **OK** to save the VLAN interface security configuration changes.

Click **Reset** to revert to the last saved configuration, or click **Exit** to close the screen without saving any updates.

Profile Overrides - Dynamic Routing Configuration (AP Only)

To define new dynamic routing settings or apply overrides to existing settings on a VLAN interface:

1 To define new security settings or apply overrides to existing settings on a VLAN interface:

The VLAN interface dynamic routing screen displays.

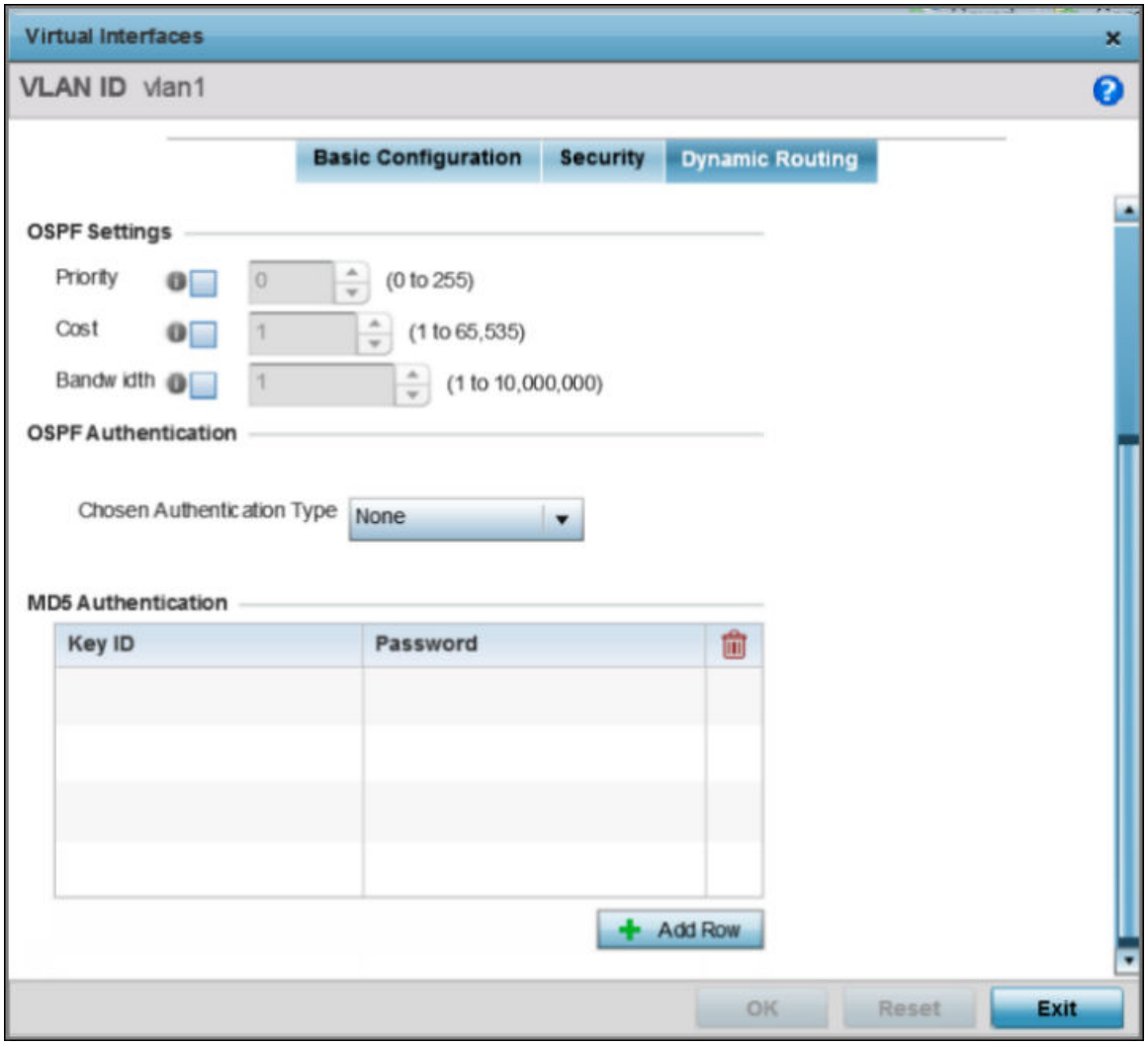



**Figure 158: Profile Overrides - Interface - VLAN Interface - Dynamic Routing Screen**

2 Define or override the following parameters in the OSPF Settings field:

| | |
|---|---|
| Priority | Select this option to enable or disable OSPF priority settings. Use the spinner to configure a value from 0 - 255. This option sets the priority of this interface becoming the Designated Router (DR) for the network. DRs provide routing updates to the network by maintaining a complete topology table of the network and sends the updates to the other routers in the network using multicast. Setting a high value increases the chance of this interface becoming a DR. Setting this value to zero prevents this interface from being elected a DR. |
| Cost | Select this option to enable or disable OSPF cost settings. Use the spinner to configure a cost value from 1 - 65535. Use this option to set the OSPF cost of this interface. OSPF cost is the overhead required to send a packet over this interface. |
| Bandwidth | Set the OSPF bandwidth from 1 - 10,000,000 KBps. |

3 In the OSPF Authentication field, use the Chosen Authentication Type drop-down list to select the authentication type used to validate credentials within the OSPF dynamic route.

The available options are **`None`**, **`null`**, **`simple-password`**, and **`message-digest`**.

4 In the MD5 Authentication table, select **+ Add Row** and add the following MD5 authenticator credentials.

| | |
|---|---|
| Key ID | Set the unique MD5 Authentication key ID. The available key ID range is 1 - 255. |
| Password | Set the OSPF password. This value is displayed as “asterisk” (*). |

Use the spinner control to set the OSPF message digest authentication key ID. The available range is from 1 - 255. The password is the OSPF key either displayed as series or asterisks or in plain text (by selecting **Show**).

5 Click **OK** to save the VLAN interface dynamic routing configuration changes.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Port Channels

The access point’s profile can be applied to customize the port channel configurations as part of its interface configuration.

Note

WiNG 7.1 does not provide port-channel configuration on AP505 and AP510 model access points.

To review an access point's existing VLAN configurations

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Interface** and select **Port Channels**.

The existing port channel configurations are displayed.

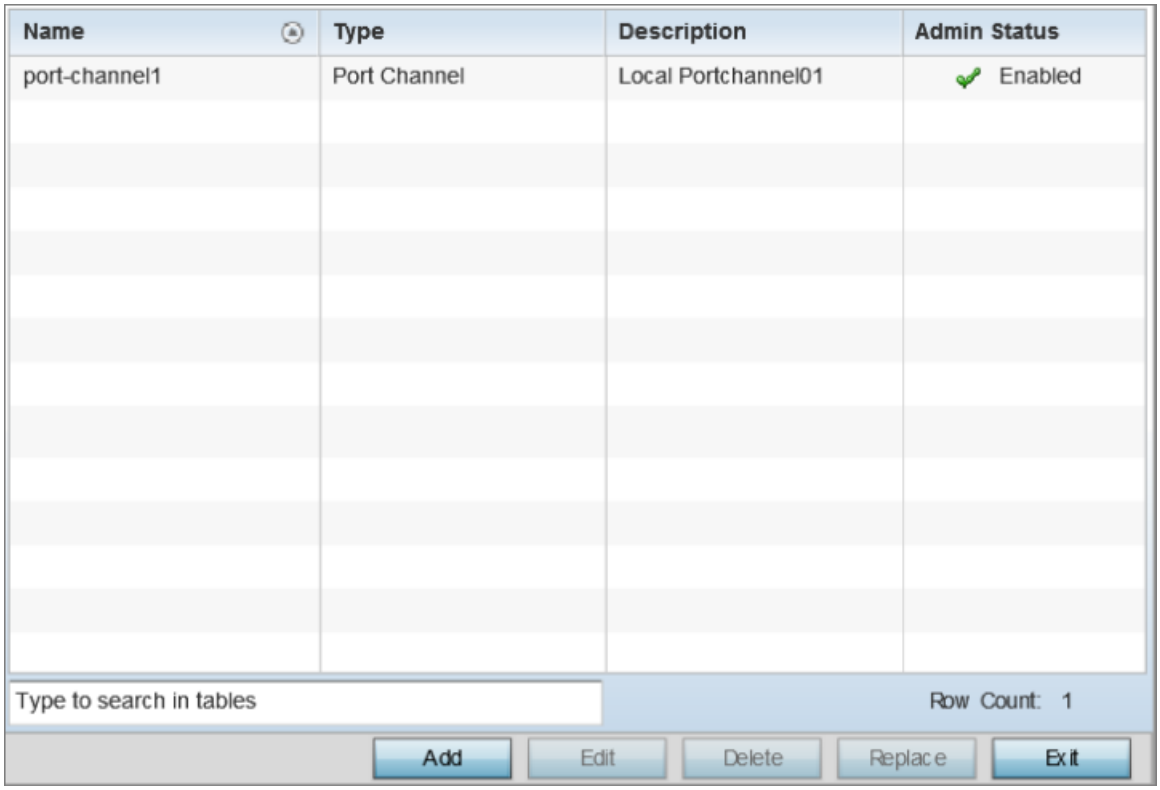



**Figure 159: Profile Overrides - Interface - Port Channels - Main Screen**

4 Review existing port channel configurations and their status to determine whether a parameter requires an override.

| | |
|---|---|
| Name | The port channel's numerical identifier assigned when it was created. The numerical name cannot be modified as part of the edit process. |
| Type | Whether the type is port channel. |
| Description | A short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations. |
| Admin Status | A green check mark means the listed port channel is active and currently enabled with the profile. A red “X” means the port channel is currently disabled and not available for use. The interface status can be modified with the port channel configuration as required. |

Profile Overrides - Basic Configuration (AP Only)

To add a new port channel configuration or apply overrides to an existing configuration:

1 Click **Add** to add a new configuration, or select an existing port channel and click **Edit**.

The port channel Basic Configuration screen displays by default.

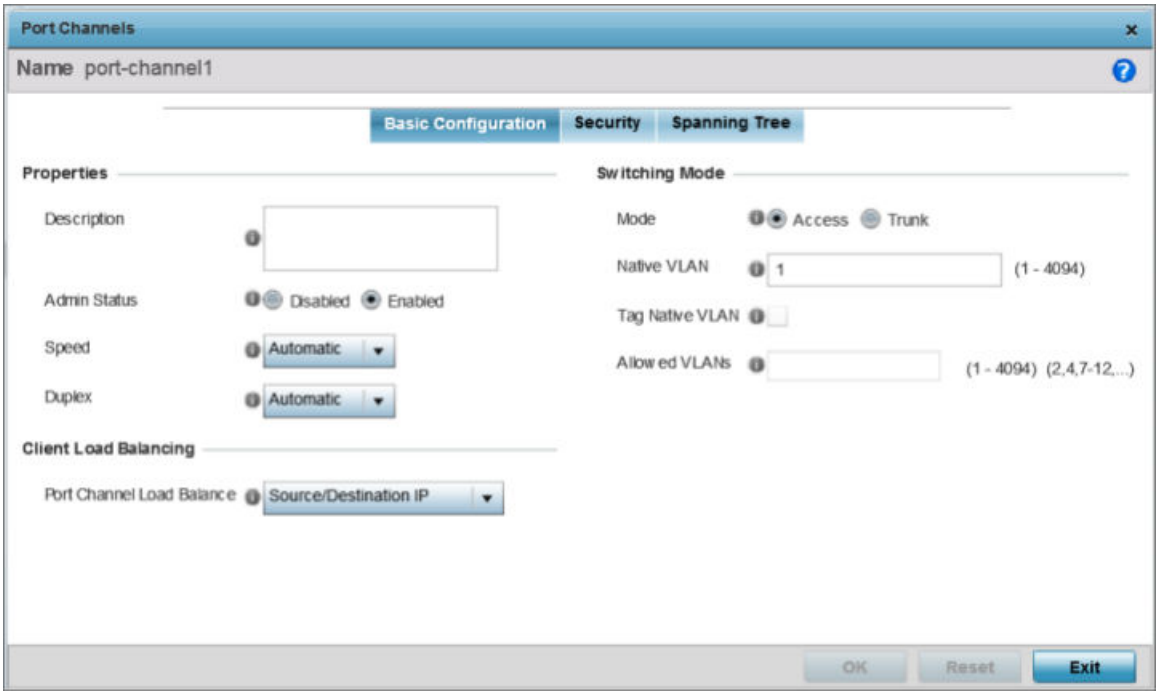



**Figure 160: Port Channel Interface - Basic Configuration Screen**

2 Set or override the following port channel Properties:

| | |
|---|---|
| Description | Enter a brief description for the port channel (64 characters maximum). The description should reflect the port channel's intended function. |
| Admin Status | Select **Enabled** to define this port channel as active to the profile it supports. Select **Disabled** to disable this port channel configuration in the profile. It can be activated at any future time when needed. The default setting is *Enabled*. |
| Speed | Select the speed at which the port channel can receive and transmit data. Select either **`10 Mbps`**, **`100 Mbps`**, or **`1000 Mbps`** to establish a 10, 100, or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission. Select *Automatic* to allow the port channel to automatically exchange information about data transmission speeds and duplex capabilities. Auto negotiation is helpful in an environment where different devices are connected and disconnected on a regular basis. The default setting is *Automatic*. |
| Duplex | Select **`Half`**, **`Full`**, or **`Automatic`**. Select *Half* duplex to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time. Select *Full* duplex to transmit data to and from the port channel at the same time. Using full duplex, the port channel can send data while receiving data as well. Select *Automatic* to enable the controller or service platform to dynamically duplex as port channel performance needs dictate. The default setting is *Automatic* |

3 In the Client Load Balancing field, use the Port Channel Load Balance drop-down menu to define whether port channel load balancing is conducted using a **`Source/Destination IP`** or a **`Source/Destination MAC`**.

The default setting is *Source/Destination IP*.

4 Set or override the following Switching Mode parameters to apply to the port channel configuration:

| | |
|---|---|
| Mode | Select either **`Access`** or **`Trunk`** to set the VLAN switching mode over the port channel. If *Access* is selected, the port channel accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to *Trunk*, the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. The default setting is *Access*. |
| Native VLAN | Use the spinner control to define a numerical Native VLAN ID from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic will be directed over when using trunk mode. The default value is 1. |
| Tag Native VLAN | Select this option to tag the native VLAN. Controllers and service platforms support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, a 12-bit frame VLAN ID is added to the 802.1Q header, so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12-bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.<br><br>Note:<br>This option is enabled when the switching mode is set as **`Trunk`**. |
| Allowed VLANs | Add VLANs that exclusively send packets over the port channel.<br><br>Note:<br>This option is enabled when the switching mode is set as **`Trunk`**. |

5 Click **OK** to save port channel basic configuration changes.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Security Configuration (AP Only)

To override port channel security configurations:

1 Select the **Security** tab.

The port channel security configuration screen displays.

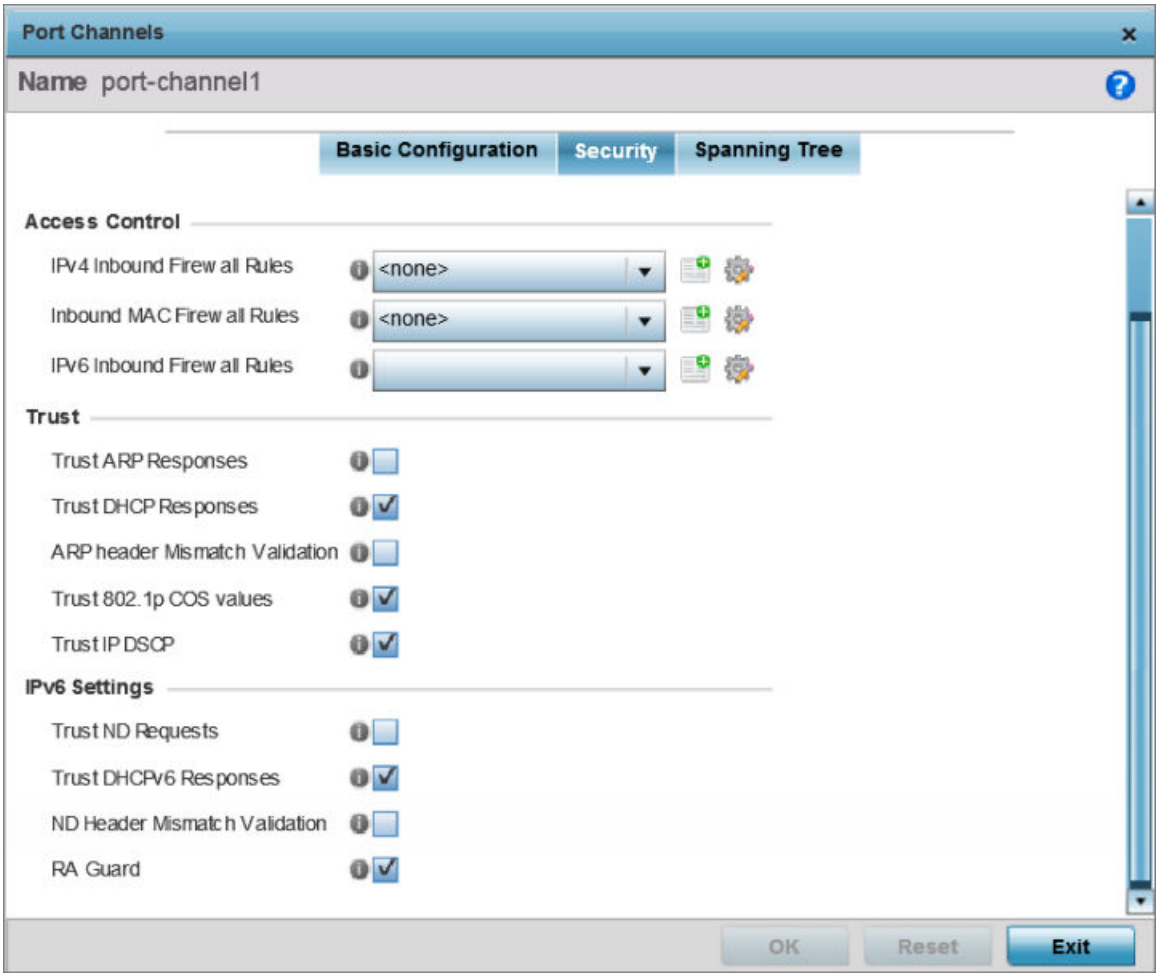



**Figure 161: Port channel - Security Configuration Screen**

2 Use the IPv4 Inbound Firewall Rules drop-down menu to select the IPv4 specific firewall rules to apply to this profile's port channel configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

3 Use the IPv6 Inbound Firewall Rules drop-down menu to select the IPv6 specific firewall rules to apply to this profile's port channel configuration.

IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

4 If there is no firewall rule that meets the data protection needs of the target port channel configuration, click the **Create** icon to define a new rule configuration, or click the **Edit** icon to modify an existing firewall rule configuration.

5 Refer to the **Trust** field to define or override the following:

| | |
|---|---|
| Trust ARP Responses | Select to enable ARP trust on this port. ARP packets received on this port are considered trusted, and the information from these packets is used to identify rogue devices within the network. This option is disabled by default. |
| Trust DHCP Responses | Select to enable DHCP trust on this port. If enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. This option is enabled by default. |
| ARP Header Mismatch Validation | Select to enable a mismatch check for the source MAC in both the ARP and Ethernet header. This option is enabled by default. |
| Trust 802.1p COS values | Select to enable 802.1p COS values on this port. This option is enabled by default. |
| Trust IP DSCP | Select this option to enable IP DSCP values on this port. This option is enabled by default. |

6 Set the following **IPv6 Settings**:

| | |
|---|---|
| Trust ND Requests | Select to enable the trust of neighbor discovery requests required on an IPv6 network. This setting is disabled by default. |
| Trust DHCPv6 Responses | Select to enable the trust all DHCPv6 responses. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network. This setting is enabled by default. |
| ND Header Mismatch Validation | Select to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This option is disabled by default. |
| RA Guard | Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This option is disabled by default. |

7 Click **OK** to save the changes and overrides to the security configuration.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Spanning Tree Configuration (AP Only)

To override port channel spanning tree configurations:

1 Select the **Spanning Tree** tab.

The port channel spanning tree configuration screen displays.

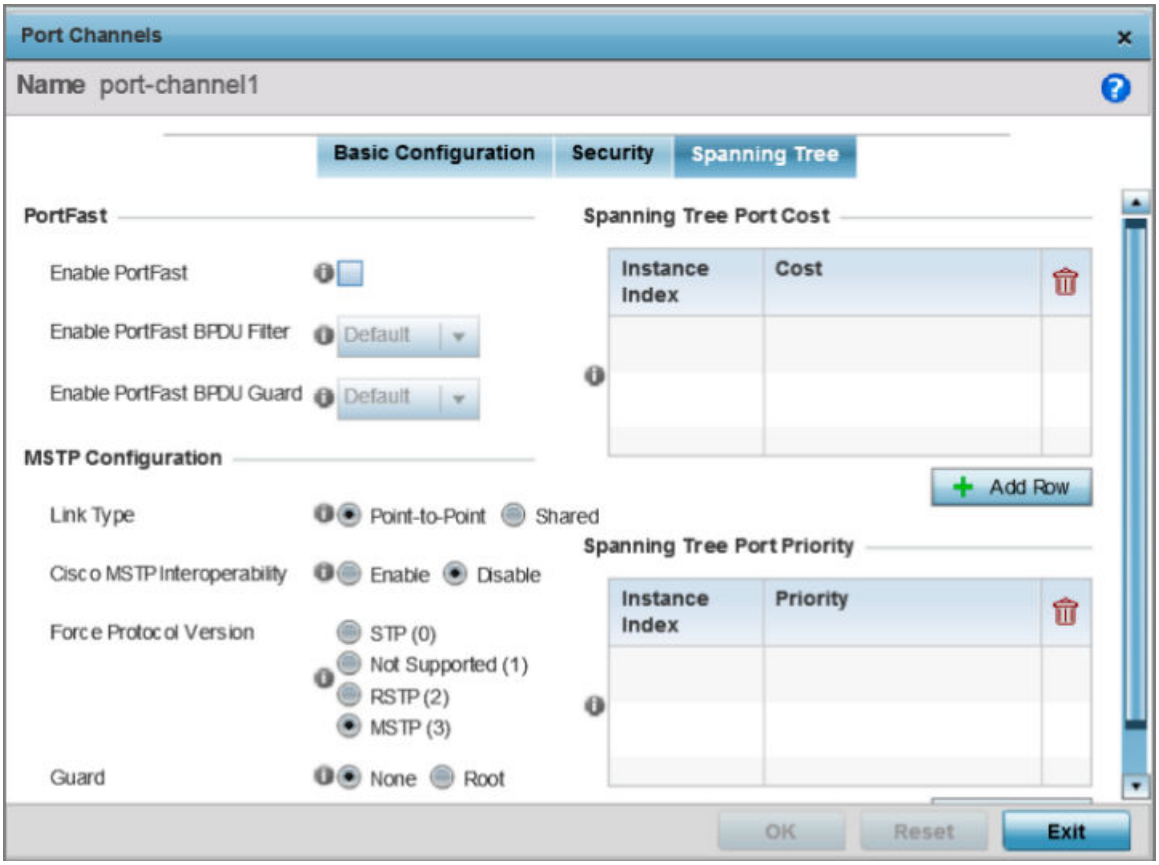



**Figure 162: Port Channel - Spanning Tree Configuration Screen**

2 Define or override the following PortFast parameters for the port channel's MSTP configuration:

| | |
|---|---|
| Enable PortFast | Select to enable drop-down menus for the Enable PortFast BPDU Filter and Enable PortFast BPDU Guard options. This option is disabled by default.<br>PortFast reduces the time required for a port to complete a MSTP state change from Blocked to Forward. PortFast must only be enabled on ports on the wireless controller directly connected to a server/workstation and not another hub or controller. PortFast can be left unconfigured on an access point. |
| Enable PortFast BPDU Filter | Enable PortFast to invoke a BPDU filter for this portfast enabled port channel. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. The options are:<br>• Default — This is the default setting. This option makes the bridge BPDU filter value to take effect.<br>• Enable — Enables BPDU filtering.<br>• Disable — Disables BPDU filtering. |
| Enable PortFast BPDU Guard | Enable PortFast to invoke a BPDU guard for this portfast enabled port channel. Enabling the BPDU guard feature means this port will shutdown on receiving a BPDU. Hence no BPDUs are processed. The options are:<br>• Default — This is the default setting. This option makes the bridge BPDU guard value to take effect.<br>• Enable — Enables shutting down of port.<br>• Disable — Disables shutting down of port. |

3 Set or override the following MSTP Configuration parameters for the port channel:

| | |
|---|---|
| Link Type | Select one of the following link type options:<br>• **Point-to-Point** - Select to configure the port as connected to a point-to-point link.<br>• **Shared** - Select to configure the port as having a shared connection.<br><br>Note:<br>A port connected to a hub is on a Shared link. Whereas, a port connected to a controller or service platform is a Point-to-Point link.<br><br>Point-to-Point is the default setting. |
| Cisco MSTP Interoperability | Select to **Enable** or **Disable** interoperability with Cisco's version of MSTP over the port. Cisco's version of MSTP is incompatible with standard MSTP. This default setting is *Disable*. |
| Force Protocol Version | Set the protocol version to either **STP(0)**, **Not Supportedd(1)**, **RSTP(2)**, or **MSTP(3)**. The default setting is *MSTP(3)*. |
| Guard | Determines whether the port channel enforces root bridge placement. Setting the guard to **Root** ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position. |

4 Refer to the Spanning Tree Port Cost table.

Define or override an Instance Index using the spinner control, and set its corresponding cost in the Cost column. The default path cost depends on the user defined port speed. The cost helps determine the role of the port channel in the MSTP network.

The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, higher the cost.

**Table 5: Spanning Tree Port Cost**

| Speed | Default Path Cost |
|---|---|
| <=100,000 bits/sec | 200000000 |
| <=1,000,000 bits/sec | 20000000 |
| <=10,000,000 bits/sec | 2000000 |
| <=100,000,000 bits/sec | 200000 |
| <=1,000,000,000 bits/sec | 20000 |
| <=10,000,000,000 bits/sec | 2000 |
| <=100,000,000,000 bits/sec | 200 |
| <=1,000,000,000,000 bits/sec | 20 |
| >1,000,000,000,000 bits/sec | 2 |

Select **+ Add Row** as needed to include additional indexes.

5 Refer to the Spanning Tree Port Priority table.

Define or override an Instance Index using the spinner control, then set the Priority. The lower the priority, the greater likelihood of the port becoming a designated port.

Select **+ Add Row** as needed to include additional indexes.

6 Click **OK** to save the changes and overrides made to the Ethernet port's Spanning Tree configuration.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Radios

An access point can have its radio profile configuration overridden after its radios have successfully associated to the network.

To review an access point's existing radio configurations

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Interface** and select **Radios**.

The selected access points radio configurations are displayed.

Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

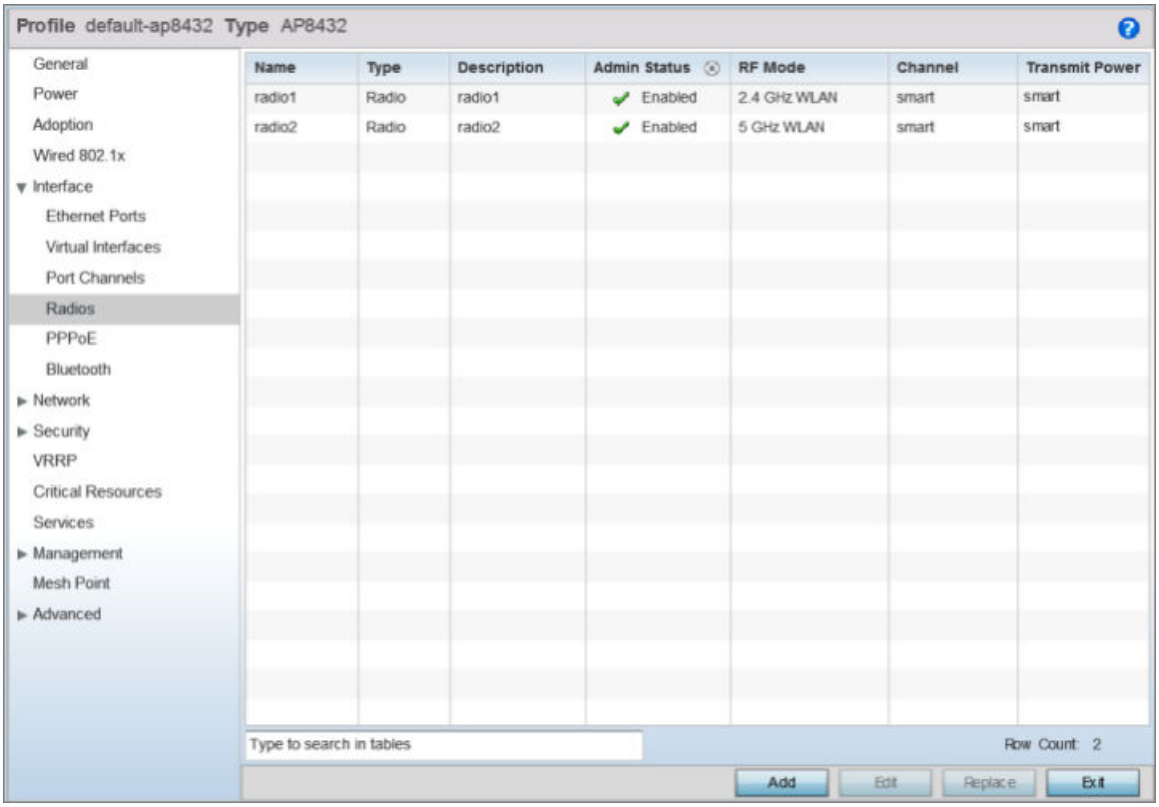



**Figure 163: Profile Overrides - Interface - Radios - Main Screen**

4 Review the following radio configuration data to determine whether a radio configuration needs to be modified to better support the network:

| | |
|---|---|
| Name | Displays whether the reporting radio is radio 1, radio 2 or radio 3. |
| Type | Displays whether the radio has been designated as a typical WLAN radio or if the radio has been designated as a sensor. |
| Description | A brief description provided by the administrator when the radio's configuration was added or modified. |
| Admin Status | A green check mark means the radio is enabled for client or sensor support. A red “X” means the radio is currently disabled. |

| | |
|---|---|
| RF Mode | Displays whether each listed radio is operating in the 802.11a/n or 802.11b/g/n radio band. If the radio is a dedicated sensor, it will be listed as a sensor to define the radio as not providing typical WLAN support. If the radio is a client bridge, it provides a typical bridging function and does not provide WLAN support. The radio band is set in the Radio Settings tab. |
| Channel | Lists the channel setting for the radio. **Smart** is the default setting. Smart indicates the acces spoint is set for dynamic Smart RF support. If set to *Smart*, the access point scans non-overlapping channels listening for beacons from other access points. After the channels are scanned, it selects the channel with the fewest access points. In the case of multiple access points on the same channel, it selects the channel with the lowest average power level. |
| Transmit Power | Lists the transmit power for each radio. The column displays **smart** if Smart-RF is used to set the transmit power for this radio. |
| Overrides | Click **Clear** to clear overrides made to this radio interface. This field is blank if there are no overrides for this radio. |

Profile Overrides - Radio Settings

To override a radio's basic settings:

1 Select the desired radio from the displayed list and click **Edit**.

The Radio Settings tab displays by default.

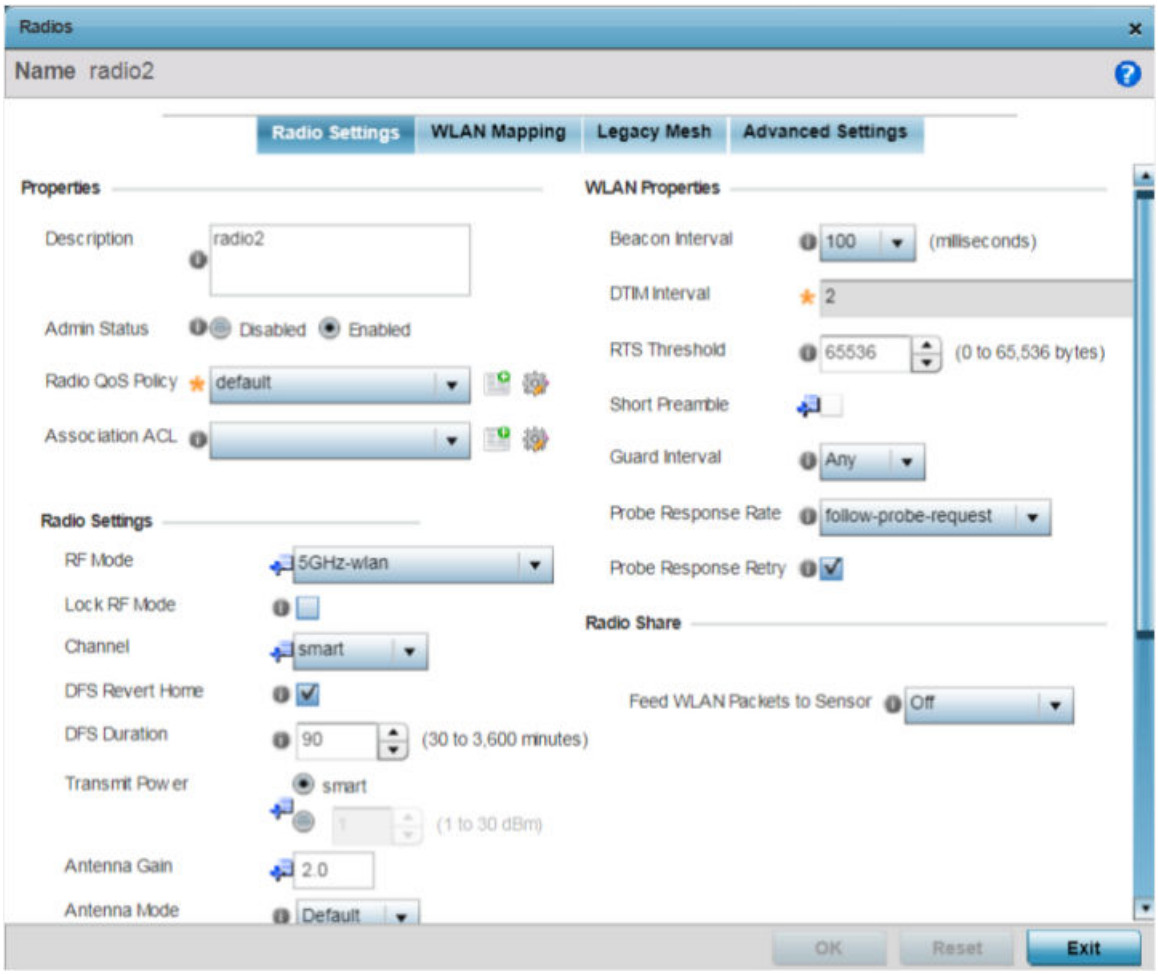



**Figure 164: Radio Interface - Radio Settings Screen**

2 Define or override the following radio configuration Properties:

| | |
|---|---|
| Description | Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations. |
| Admin Status | Select **`Enabled`** or **`Disabled`** to define this radio's current status within the network. When enabled, the access point is operational and available for client support within the network. The radio is enabled by default and must be shut down manually. |

| | |
|---|---|
| Radio QoS Policy | Use the drop-down menu to specify an existing QoS policy to apply to the access point radio in respect to its intended radio traffic. If no existing policy is suitable for this radio's intended operation, select the **Create** icon to define a new QoS policy. |
| Association ACL | Specify an existing Association ACL policy to apply to the radio. An Association ACL is a policy-based ACL *(Access Control List)* that either prevents or allows wireless clients from connecting to an access point radio. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the fields in the packet are compared to applied ACLs to verify the packet has the required permissions needed to be forwarded. If a packet does not meet any of the ACL criteria, the packet is dropped. Select the **Create** icon to define a new Association ACL. |

3 Define or override the following Radio Settings for the selected access point radio:

| | |
|---|---|
| RF Mode | The radio can be configured to provide WLAN service for 2.4 GHz and 5 GHz enabled clients. You can also set the radio to provide sensor support, scan-ahead support, or function as a client bridge.<br>Set the mode to either *2.4 GHz WLAN* or *5 GHz WLAN* depending on the radio's intended client support requirement.<br>Set the mode to *Sensor* if using the radio for rogue device detection. To set a radio as a detector, disable Sensor support on the other access point radio.<br>Set the mode to *scan-ahead* in DFS aware countries to allow a mesh points secondary radio to scan for an alternative channel for backhaul transmission in the event of a radar event on the principal radio. The secondary radio is continually monitoring the alternate channel, which means the principal radio can switch channels and transmit data immediately without waiting for the channel availability check.<br>Set the mode to *bridge* to configure the radio as a client bridge. A client bridge enables the access point to connect to a third party access point and bridge frames to it.<br>The client-bridge is supported only on the following access point models: AP6522, AP6562, AP7522, AP7532, AP7602, AP7612, AP7622, AP7632 and AP7622<br><br>Note: For AP510 model access point, you can provide 5 GHz WLAN support on both radio 1 and radio 2.<br><br>Note: rf-mode *scan-ahead* and *bridge* are not supported on the AP 505i and AP510i model access points.<br><br>Note: For information on the possible modes of operations for AP505 and AP510 radios, see ap510i and ap505i. |
| Lock RF Mode | Select this option to lock Smart RF calibration functions for this radio. The default setting is disabled. |
| Channel | Select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select **Smart** for the radio to scan non-overlapping channels to listen for beacons from other access points. After channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it selects the channel with the lowest average power level. The default value is Smart.<br>Channels with a "w" appended to them are unique to the 40 MHz band. |

| | |
|---|---|
| DFS Revert Home | Select this option to enable a radio to return to its original channel. DFS *(Dynamic Frequency Selection)* prevents a radio from operating in a channel where radar signals are present. When radar signals are detected in a channel, the radio changes its channel of operation to another channel. The radio cannot use the channel it has moved from for the next 30 minutes. When DFS Revert Home is selected, the radio can return back to its original channel of operation when the 30-minute period is over. When not selected, the radio cannot return back to its original channel of operation ever after the mandatory 30-minute evacuation period is over.<br><br>Note:<br>This option is enabled only if the RF Mode is set to 5GH-wlan. |
| DFS Duration | Set the DFS duration between 30 and 3,600 minutes. This is the duration for which the radio stays in the new channel. The default value is 90 minutes. |
| Transmit Power | Set the transmit power of the selected access point radio. If the access point has two radios, each radio should be configured with a unique transmit power in respect to its intended client support function.<br>Select **smart** to let Smart RF determine the transmit power. Or else, select the other option and manually enter the radio's transmit power. The default setting is smart.<br><br>Note:<br>This option is enabled only if the RF Mode is set to 2.5GHZ-wlan or 5GH-wlan. |
| Antenna Gain | Set the antenna between 0.00 - 15.00 dBm. The access point's PMACF *(Power Management Antenna Configuration File)* automatically configures the access point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00. |
| Antenna Mode | Set the number of transmit and receive antennas on the access point. 1x1 is used for transmissions over just the single "A" antenna, 1x3 is used for transmissions over the "A" antenna and all three antennas for receiving. 2x2 is used for transmissions and receipts over two antennas for dual antenna models. The default setting is dynamic, based on the access point model and its transmit power settings. |
| Enable Antenna Diversity | Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default. |
| Adaptivity Recovery | Select this option to switch channels when an access point's radio is in adaptivity mode. In adaptivity mode, an access point monitors interference on its set channel and stops functioning when the radio's defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default. |

| | |
|---|---|
| Adaptivity Timeout | Set the adaptivity timeout from 30 to 3,600 minutes. The default setting is 90 minutes. |
| Wireless Client Power | Select this option to enable a spinner control for client radio power transmissions in dBm. The available range is 0 - 20 dBm. This option is disabled by default. |
| Dynamic Chain Selection | Select this option to allow the access point radio to dynamically change the number of transmit chains. The radio uses a single chain/antenna for frames at non 802.11n data rates. This setting is disabled by default. |
| Data Rate | Once the radio band is provided, the **Rate** drop-down menu populates with rate options depending on the 2.4 or 5.0 GHz band selected.<br><br>Note:<br>The Data Rates drop-down menu is disabled for radios running as sensors.<br><br>If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5.0 GHz is selected as the radio band, select separate 802.11a and 802.11n rates define how they are used together. When using 802.11n (in either the 2.4 or 5.0 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).<br>If you are dedicating the radio to either 2.4 or 5 Ghz support, a **Custom Rates** option is available to set a modulation and coding scheme (MCS) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). If **Basic** is selected within the 802.11n Rates field, the MCS0-7 option is auto selected as a supported rate and that option is grayed out. If **Basic** is not selected, any combination of MCS0-7, MCS8-15 and MCS16-23 can be supported, including a case where MCS0-7 and MCS16-23 are selected and not MCS8-15. The MCS0-7 and MCS8-15 options are available to each support access point.<br><br>Note: For information on supported data rates, click here. |
| Radio Placement | Specify whether the radio is located **Indoor** or **Outdoor**. The placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions. The default setting is Indoors. |

| | |
|---|---|
| Max Clients | Set the maximum permissible client connections for this radio. Set a value from 0 - 256. The default value is 256.<br><br>Note:<br>Most access point models can support up to 256 clients per access point radio.<br><br>Note: The AP505i and AP510i can support a mximum of 250 clients per radio. |
| Rate Selection Methods | Specify the algorithm to use for rate selection. Select Standard to use the standard rate selection algorithm. Select Opportunistic to use the Opportunistic rate selection algorithm. |

4 Set or override the following WLAN Properties for the selected access point radio:

| | |
|---|---|
| Beacon Interval | Set the interval between radio beacons in milliseconds (either 50, 100 or 200). A beacon is a packet broadcast by adopted radios to keep the network synchronized. Included in a beacon is the WLAN service area, radio address, broadcast destination addresses, a time stamp, and indicators about traffic and delivery (such as a DTIM). Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jittersensitive. The default value is 100 milliseconds. |
| DTIM Interval | Set a DTIM Interval to specify a period for DTIM *(Delivery Traffic Indication Messages)*. A DTIM is periodically included in a beacon frame transmitted from adopted radios. The DTIM indicates broadcast and multicast frames (buffered at the access point) are soon to arrive. These are simple data frames that require no acknowledgment, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive. |

| | |
|---|---|
| RTS Threshold | Specify a RTS *(Request To Send)* threshold (from 1 - 65,536 bytes) for use by the WLAN's adopted access point radios. RTS is a transmitting station's signal that requests a CTS *(Clear To Send)* response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path. The default value is 65,536 bytes.<br>Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/ CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.<br>Consider the tradeoffs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.<br>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold. |
| Short Preamble | If you are using an 802.11bg radio, select this option for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This option is disabled by default. |
| Guard Interval | Specify a **`Long`** or **`Any`** guard interval. The guard interval is the space between characters being transmitted. The guard interval eliminates ISI *(inter-symbol interference)*. ISI occurs when echoes or reflections from one character interfere with another character. Adding time between transmissions allows echo's and reflections to settle before the next character is transmitted. A shorter guard interval results in shorter character times which reduces overhead and increases data rates by up to 10%. The default value is *Any*. |
| Probe Response Rate | Specify the data rate used for the transmission of probe responses. Options include **`highest-basic`**, **`lowest-basic`**, and **`follow-probe-request`**. The default value is follow-probe-request. |
| Probe Response Retry | Select this option to retry probe responses if they are not acknowledged by the target wireless client. This option is enabled by default. |

5 Use the **Feed WLAN Packets to Sensor** drop-down menu to allow the radio to send WLAN packets to the sensor radio.

Options include **`Off`**, **`Inline`**, and **`Promiscuous`**. The default setting is Off.

Profile Overrides - Wlan/Mesh Mapping

You can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

**Note**

WiNG 7.1 release does not support MeshConnex on AP505i and AP510i model access points. This option will be supported in future releases.

To override a radio's WLAN/Mesh assignment:

1 Select the **WLAN Mapping / Mesh Mapping** tab.

The WLAN / Mesh Mapping screen displays.

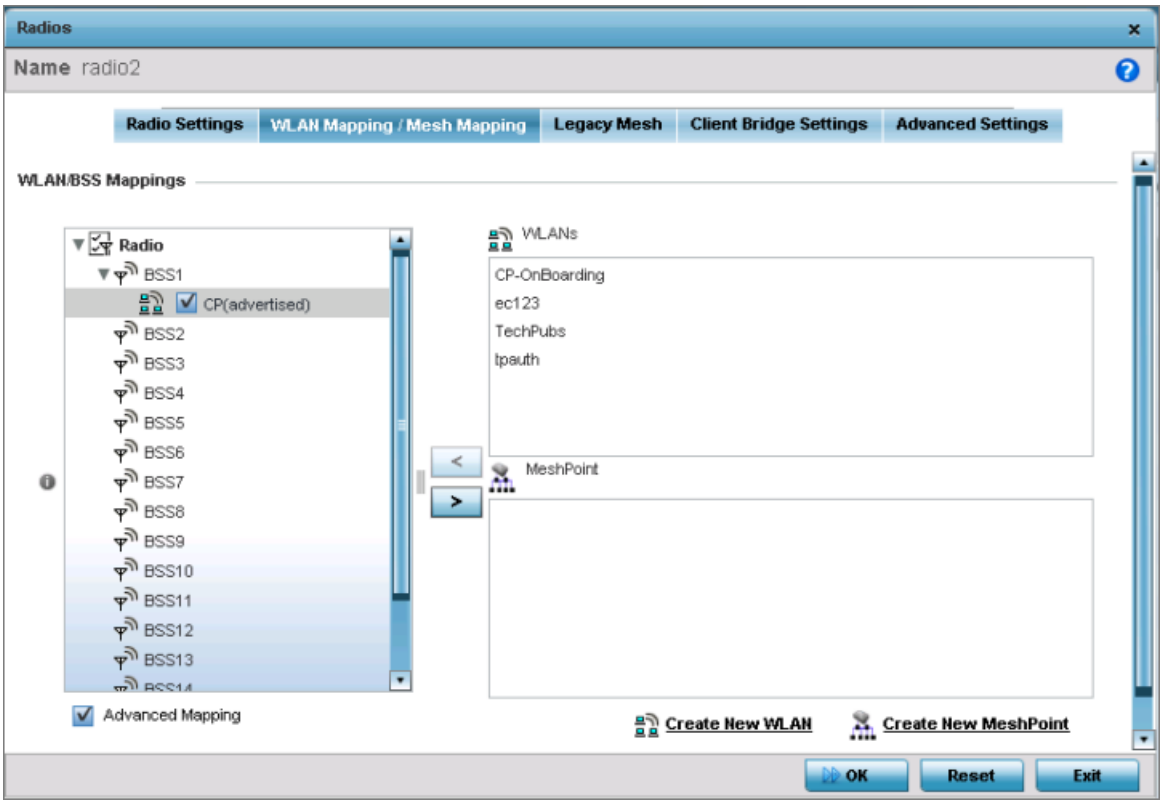



**Figure 165: Profile Overrides - Radio Interface - WLAN Mapping / Mesh Mapping Screen**

2 Refer to the WLAN/BSS Mappings field to set or override WLAN BSSID assignments for an existing access point deployment.

Use the '<' or '>' buttons to assign WLANs and mesh points to the available BSSIDs.

Administrators can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio. Each supported access point model can support up to 8 BSS IDs.

3 Select **Advanced Mapping** to populate the Radio field with BSS IDs.

4 Click **OK** to save the changes and overrides to the WLAN mapping.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Legacy Mesh

Each radio profile can have a unique mesh mode and link configuration. This provides a customizable set of connections to other mesh supported radios within the same radio coverage area.

**Note**

WiNG 7.1 release does not support MeshConnex on AP505i and AP510i model access points. This feature will be supported in future releases.

To override a radio's Legacy Mesh configuration:

1 Select the **Legacy Mesh** tab.

The Legacy Mesh screen displays. Use this screen to define or override how mesh connections are established and the number of links available among access points within the Mesh network.

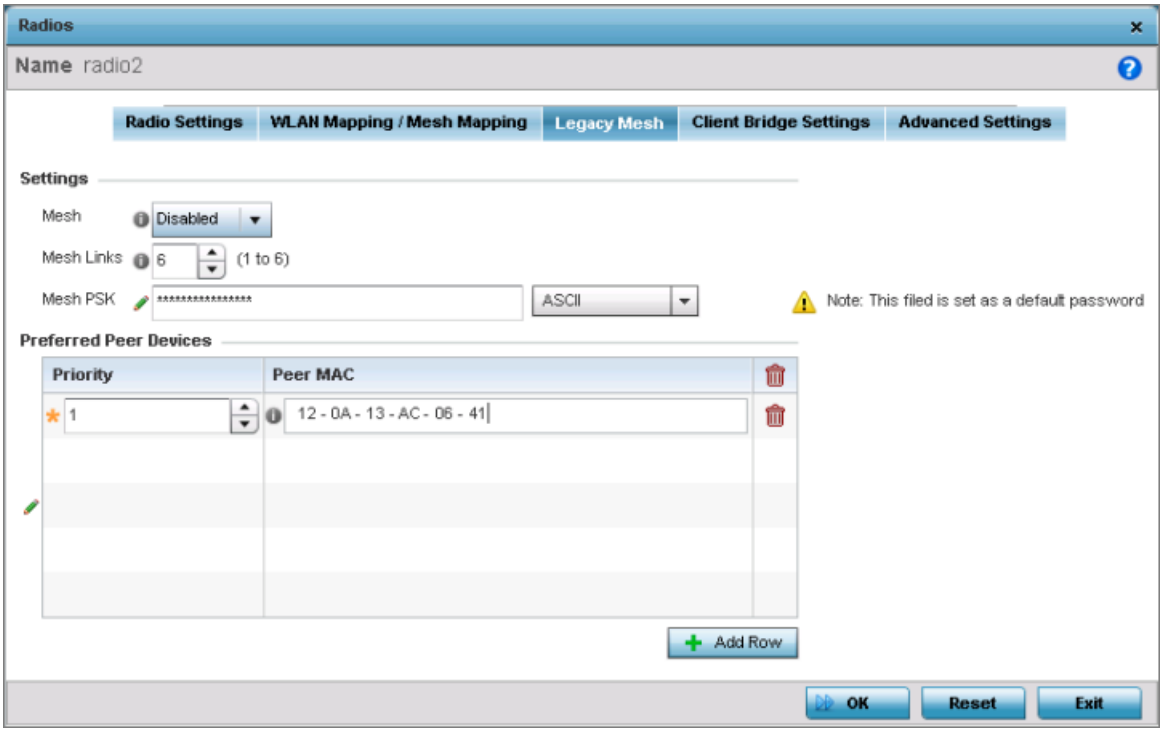



**Figure 166: Radio Interface - Legacy Mesh Configuration Screen**

2 Define the following mesh legacy **Settings**:

| | |
|---|---|
| Mesh | Set the mesh mode for this radio – either **`Client`**, **`Portal`**, or **`Disabled`**. Select *Client* to scan for mesh portals, or nodes that have connection to portals, and connect through them. The *Portal* operation begins beaconing immediately and accepts connections from other mesh supported nodes. In general, the portal is connected to the wired network. The default value is *Disabled*. |
| Mesh Links | Specify the number of mesh links (1 -6) an access point radio will attempt to create. The default setting is 3 links. |
| Mesh PSK | Use the field to define the shared key for mesh. From the drop-down, select the type of the key. Click **Show** to display the characters used in the key. |

3 In the Preferred Peer Devices table, click **+ Add Row** and define the following MAC addresses to preferred mesh connection mappings:

| | |
|---|---|
| Priority | Use this spinner control to set a priority (1 -6) for connection preference. |
| Peer MAC | For each priority value, define the MAC address of the associated peer device. Use this option to are define MAC addresses representing peer devices for the radio to connect to in mesh mode. |

4 Click **OK** to save the Mesh configuration changes.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Client Bridge

An access point's radio can be configured to form a bridge between its wireless/wired clients and an infrastructure WLAN. The bridge radio authenticates and associates with an infrastructure WLAN access point. After successful association, the access point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, thereby providing the clients access to the infrastructure WLAN resources.

Note

WiNG 7.1 release does not support Client Bridge configuration on AP505i and AP510i model access points. This feature will be supported in future releases.

To override a radio's client bridge settings:

1 Select the **Client Bridge Settings** tab.

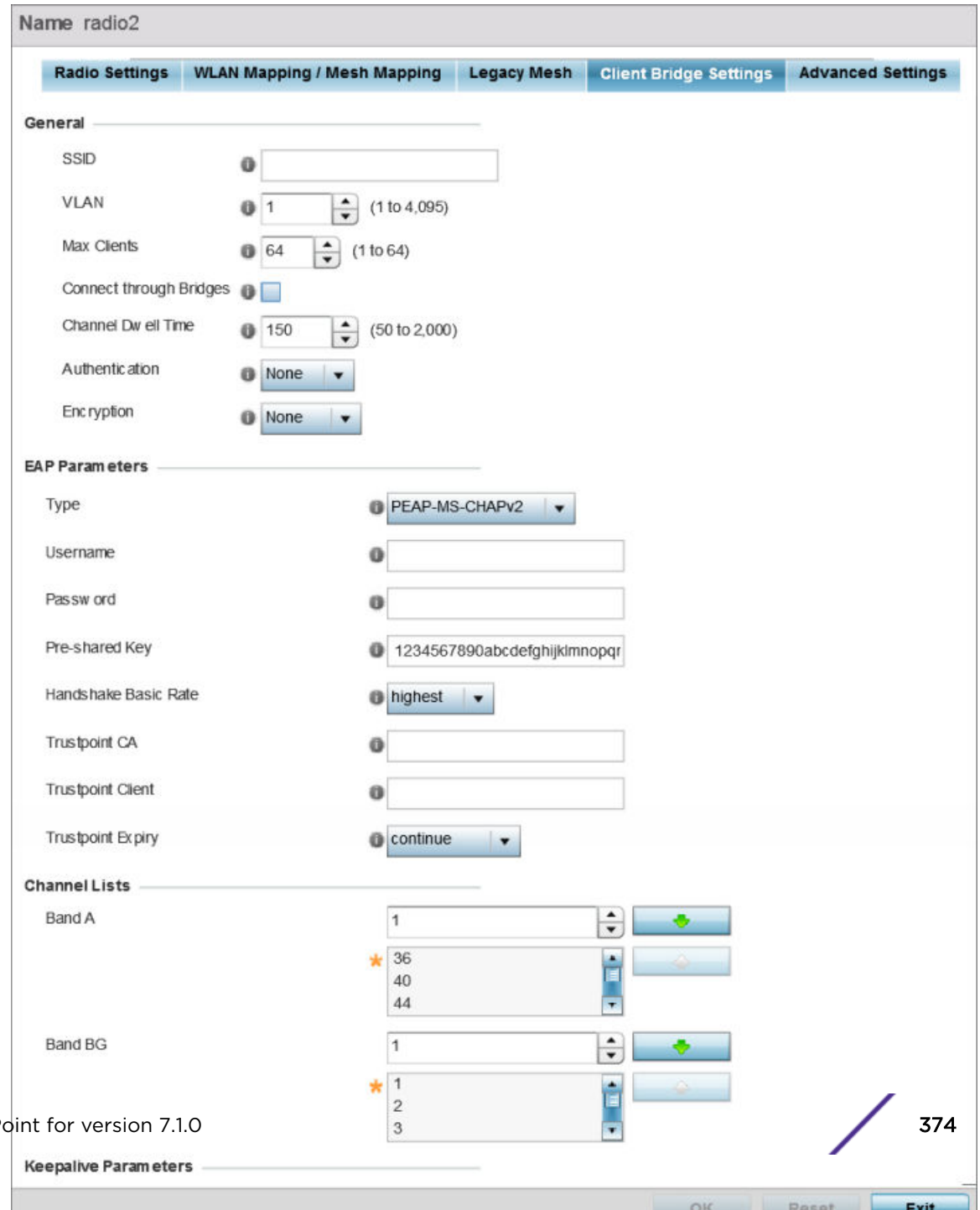
Note

Before configuring the client-bridge parameters, set the radio's rf-mode to **bridge**.

An access point's radio can be configured to form a bridge between its wireless/wired clients and an infrastructure WLAN. The bridge radio authenticates and associates with an infrastructure WLAN Access Point. After successful association, the Access Point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, thereby providing the clients access to the infrastructure WLAN resources.

This feature is supported only on the AP6522, AP6562, AP7522, AP7532, AP7562, AP7602, AP7622.

The selected radio's client bridge configuration screen displays.



2 Define the following General settings:

| | |
|---|---|
| SSID | Set the infrastructure WLAN's SSID, with which the client-bridge access point associates. |
| VLAN | Set the VLAN to which the bridged clients' sessions are mapped after successful association with the infrastructure WLAN. Once mapped, the client bridge communicates with permitted hosts over the infrastructure WLAN. Specify the VLAN from 1 to 4095. |
| Max Clients | Set the maximum number of client-bridge access points that can associate with the infrastructure WLAN. Specify a value from 1 to 64. The default value is 64. |
| Connect through Bridges | Select this option to enable the client-bridge access point radio to associate with the infrastructure WLAN through another client-bridge radio thereby forming a chain. This is referred to as daisy chaining of client-bridge radios. This option is disabled by default. |
| Channel Dwell Time | Set the channel-dwell time from 50 to 2000 milliseconds. This is the time the client-bridge radio dwells on each channel (configured in the list of channels) when scanning for an infrastructure WLAN. The default is 150 milliseconds. |
| Authentication | Set the mode of authentication with the infrastructure WLAN. The authentication mode specified here should be the same as that configured on the infrastructure WLAN. The options are **None** and **EAP**. If you select **EAP**, specify the EAP authentication parameters. The default setting is *None*.<br>For information on WLAN authentication, see Configuring WLAN Security on page 556. |
| Encryption | Set the packet encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are **None**, **CCMP**, and **TKIP**. The default setting is *None*.<br>For information on WLAN encryption, see Configuring WLAN Security on page 556. |

3 Refer to the **EAP Parameters** field and define the following EAP authentication parameters:

| | |
|---|---|
| Type | Select the EAP authentication method used by the supplicant. The options are **TLS** and **PEAP-MS-CHAPv2**. The default EAP type is **PEAP-MS-CHAPv2**. |
| Username | Set the 32-character maximum user name for an EAP authentication credential exchange. |
| Password | Set the 32-character maximum password for the specified EAP user name. |
| Pre-shared Key | Set the PSK *(pre-shared key)* used with EAP. Note that the authenticating algorithm and PSK should be the same as on the infrastructure WLAN. |
| Handshake Basic Rate | Set the basic rate of exchange of handshake packets between the client-bridge and infrastructure WLAN Access Points. The options are **highest** and **normal**. The default value is **highest**. |

| | |
|---|---|
| Trustpoint CA | Set the *Trustpoint CA* name (this is the trustpoint installed on the RADIUS server host). This parameter is applicable to both EAP-TLS and PEAP-MS-CHAPv2 authentication modes.<br>In case of both EAP-TLS and PEAP-MS-CHAPv2 authentication, provide the RADIUS server TP name to enable RADIUS server certificate validation at the client end. This parameter is not mandatory for enabling TP-based authentication of CB *(Client-Bridge)* AP. |
| Trustpoint Client | Set the *Trustpoint Client* name (this is the TP installed on the CB AP). This parameter is applicable only for EAP-TLS authentication mode. When configured, this client certificate is sent across a TLS tunnel and matched for authentication at the RADIUS server host. This configuration is mandatory for enabling TP-based authentication of CB AP. |
| Trustpoint Expiry | Use the drop-down menu to specify whether the wireless client-bridge is to be continued or discontinued in case of certificate expiry.<br>In EAP-TLS authentication, a CA-signed certificate is used to authenticate the CB AP and RADIUS server host to establish the wireless CB. Use this option to specify whether the wireless CB is to be continued or terminated on expiration of this certificate.<br>**`continue`** – Enables continuation of the CB even after the certificate (CA/client) has expired. When selected, this option enables automatic CA certificate deployment as and when new CA certificates are available. This is the default setting.<br>**`discontinue`** – Terminates the CB once the certificate (CA/client) has expired.<br><br>Note:<br>Configure this parameter only if the CB AP and the RADIUS server host are using a crypto CMP policy for automatic certificate renewal. For more information, see Crypto CMP Policy on page 685. |

4 Refer to the **Channel Lists** field and define the list of channels the client-bridge radio scans when scanning for an infrastructure WLAN.

| | |
|---|---|
| Band A | Define a list of channels for scanning across all the channels in the 5.0 GHz radio band. |
| Band BG | Define a list of channels for scanning across all the channels in the 2.4 GHz radio band. |

5 Refer to the **Keepalive Parameters** field and define the following configurations:

| | |
|---|---|
| Keepalive Type | Set the keepalive frame type exchanged between the client-bridge and infrastructure access points. This is the type of packets exchanged between the client-bridge and infrastructure access points, at specified intervals, to keep the client-bridge link up and active. The options are **`null-data`** and **`WNMP`** packets. The default value is **`null-data`**. |
| Keepalive Interval | Set the keepalive interval from 0 to 86,400 seconds. This is the interval between two successive keepalive frames exchanged between the client-bridge and infrastructure Access Points. The default value is 300 seconds. |
| Inactivity Timeout | Set the inactivity timeout for each bridge MAC address from 0 to 864,000 seconds. This is the time for which the client-bridge access point waits before deleting a wired/wireless client's MAC address from which a frame has not been received for more than the time specified here. For example, if the inactivity time is set at 120 seconds, and if no frames are received from a client (MAC address) for 120 seconds, it is deleted. The default value is 600 seconds. |

6 Refer to the **Radio Link Behaviour** field and define the following configurations:

| | |
|---|---|
| Shutdown Other Radio when Link Goes Down | Select this option to enable shutting down of the non-client bridge radio (this is the radio to which wireless clients associate) when the link between the client-bridge and infrastructure access points is lost. When enabled, wireless clients associated with the non-client bridge radio are pushed to search for and associate with other access points having backhaul connectivity. This option is disabled by default.<br>If you enable this option, specify the time for which the non-client bridge radio is shut down. Use the spinner to specify a time from 1 - 1,800 seconds. |
| Refresh VLAN Interface when Link Comes Up | Select this option to enable the SVI to refresh on re-establishing client bridge link to the infrastructure access point. If you are using a DHCP assigned IP address, this option also causes a DHCP renew. This option is enabled by default. |

7 Refer to the **Roam Criteria** field and define the following configurations:

| | |
|---|---|
| Seconds for Missed Beacons | Set this interval from 0 to 60 seconds. This is the time for which the client-bridge access point waits, after missing a beacon from the associated infrastructure WLAN access point, before roaming to another infrastructure access point. For example, if Seconds for Missed Beacon is set to 30 seconds, and if more than 30 seconds have passed since the last beacon received from the infrastructure access point, the client-bridge access point resumes scanning for another infrastructure access point. The default value s 20 seconds. |
| Minimum Signal Strength | Set the minimum signal-strength threshold for signals received from the infrastructure access point. Specify a value from -128 to -40 dBm. If the RSSI value of signals received from the infrastructure access point falls below the value specified here, the client-bridge access point resumes scanning for another infrastructure access point. The default is -75 dBm. |

8 Click **OK** to save the changes and overrides to the client bridge settings screen.

Click **Reset** to revert to the last saved configuration.

Profile Overrides Advanced Settings

To override a radio's advanced settings:

1 Select the **Advanced Settings** tab.

The selected radio interface's advanced settings screen displays:

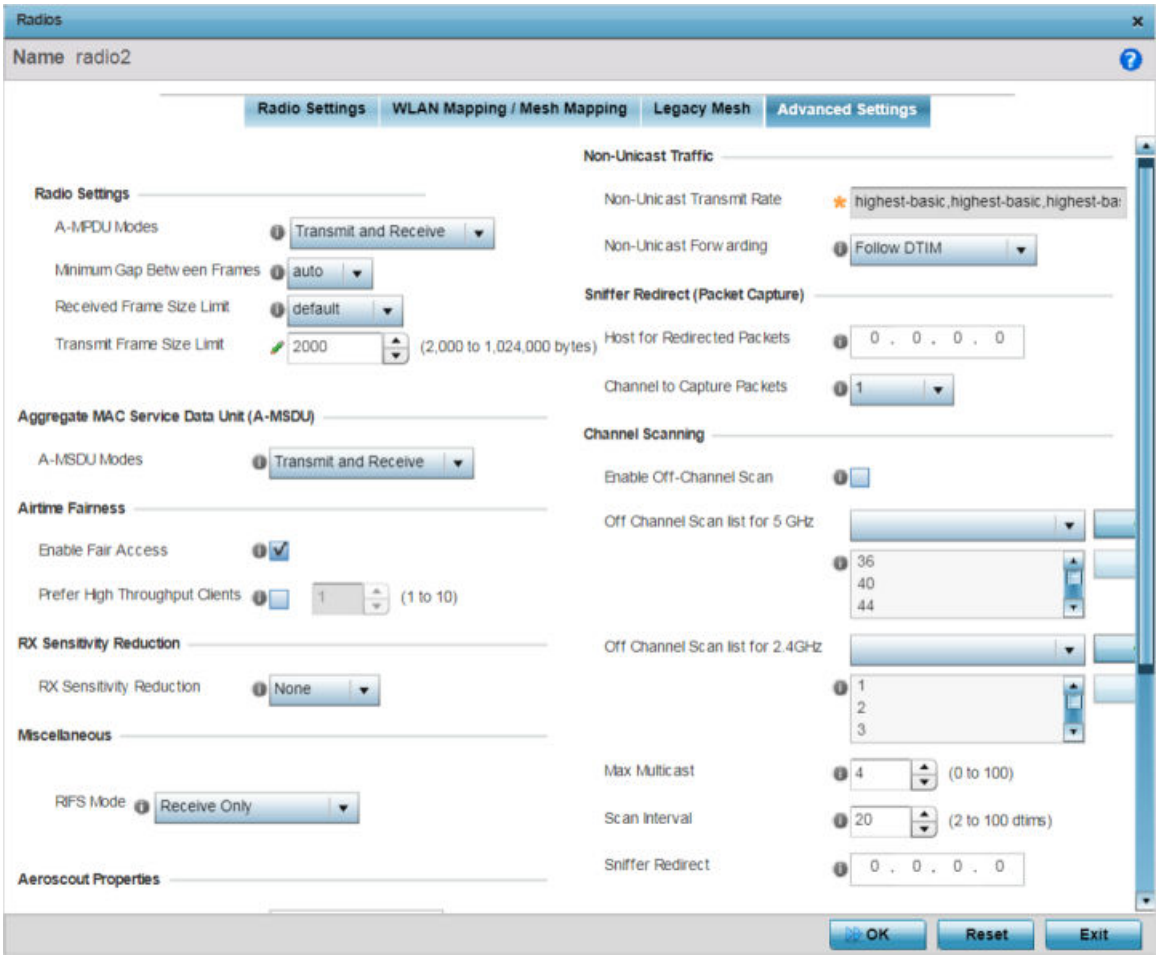



**Figure 168: Access Point - Radio Interface - Advanced Settings Screen**

2 In the Radio Settings field, define or override how MAC service frames are aggregated by the access point radio.

| | |
|---|---|
| A-MPDU Modes | Specify the A-MPDU mode. Options include **`Transmit Only`**, **`Receive Only`**, **`Transmit and Receive`**, and **`None`**. The default value is *Transmit and Receive*. Using the default value, long frames can be both sent and received (up to 64 KB). When this option is enabled, define a transmit limit, a receive limit, or both. |
| Minimum Gap Between Frames | Use the drop-down menu to define, in microseconds, the minimum gap between consecutive A-MPDU frames. The options include:<br>• **`0`** – Configures the minimum gap as 0 microseconds<br>• **`1`** – Configures the minimum gap as 1 microseconds<br>• **`2`** – Configures the minimum gap as 2 microseconds<br>• **`4`** – Configures the minimum gap as 4 microseconds<br>• **`8`** – Configures the minimum gap as 8 microseconds<br>• **`16`** – Configures the minimum gap as 16 microseconds<br>• **`auto`** – Auto configures the minimum gap depending on the platform and radio type (default setting) |

| | |
|---|---|
| Received Frame Size Limit | If the A-MPDU mode is set to *Receive Only* or *Transmit and Receive*, use this option to define an advertised maximum limit for received A-MPDU aggregated frame size. The options include:<br>• **8191** - Advertises the maximum received frame size limit as 8191 bytes.<br>• **16383** - Advertises the maximum received frame size limit as 16383 bytes.<br>• **32767** - Advertises the maximum received frame size limit as 32767 bytes.<br>• **65535** - Advertises the maximum received frame size limit as 65535 bytes.<br>• **128000** - Advertises the maximum received frame size limit as 128000 bytes.<br>• **256000** - Advertises the maximum received frame size limit as 256000 bytes.<br>• **512000** - Advertises the maximum received frame size limit as 512000 bytes.<br>• **1024000** - Advertises the maximum received frame size limit as 1024000 bytes.<br>• **default** - This option auto configures the maximum received frame size based on the platform and radio type. This is the default setting. |
| Transmit Frame Size Limit | If the A-MPDU mode is set to *Transmit Only* or *Transmit and Receive*, use the spinner control to set limit on transmitted A-MPDU aggregated frame size. The range depends on the AP type and the radio selected.<br>For 802.11ac capable APs, the range is as follows:<br>• **2000 – 65,535 bytes** - For radio 1, the range is 2000 - 65,535 bytes. The default value is 65,535 bytes.<br>Note:<br>The WiNG *AP7662* and *AP7632* access points are an exception to the above rule. For the AP7662 and AP7632 access point models, the radio 1 range is *2000 - 1,024,000 bytes*. And the default value is 1,024,000 bytes.<br>• **2000 – 1,024,000 bytes** - For radio 2, the range is 2000 - 1,024,000 bytes. The default value is 1,024,000 bytes.<br>Note:<br>The WiNG 802.11ac capable APs are: AP7522, AP7532, AP7562, AP7602, AP7612, AP7632, AP7662, AP8432, and AP8533.<br>For non 802.11ac capable APs the range is as follows:<br>• **2000 – 65,535 bytes** - For both radio 1 and radio 2 the range is 2000 - 65,535 bytes. The default value is 65,535 bytes. |

3 In the Aggregate MAC Service Data Unit (A-MSDU) field, use the A-MSDU Modes drop-down menu to set or override the supported A-MSDU mode.

Available modes are **Receive Only** and **Transmit and Receive**. Use *Transmit and Receive* to send and receive frames up to 4 KB. The buffer limit is not configurable. Transmit and Receive is the default value.

4 Use the Airtime Fairness fields to configure wireless access to devices based on their usage.

| | |
|---|---|
| Enable Fair Access | Select to enable fair access to all peer devices. |
| Prefer High Throughput Clients | Select to prefer clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/b/g) clients. Use the spinner control to set a weight for the higher throughput clients. |

5 Use the **Rx Sensitivity Reduction** drop-down menu to set the selected radio's receive sensitivity reduction threshold level.

This threshold determines the RSSI (in dBm) at which the radio acknowledges the SOP *(Start of Packet)* frames received from the client, and begins to demodulate and decode the packets.

In highly dense environments, or single-channel networks, having two or more radios sharing a channel, CCI *(co-channel interference)* adversely impacts network performance. By setting this threshold, you can control the radio's receive sensitivity to interference and noise, thereby reducing the impact of CCI. You are basically configuring the AP to not decode packets that have a signal strength below the specified threshold level.

The available *rx-sensitivity-reduction* threshold levels are: **`High`**, **`Low`**, **`Medium`** and **`None`**. Set the threshold level as *High*, to force your radio to ignore all traffic having a signal strength below the high threshold level value. This results in fewer traffic interruptions due to collision and Wi-Fi interference. Note, the default setting is *None*.

The following table provides the *rx-sensitivity-reduction threshold level* to *RSSI* mapping for the 2.4 GHz and 5 GHz bands:

| 802.11 Bands | High Threshold | Medium Threshold | Low Threshold |
|---|---|---|---|
| 2.4 GHz | -79 dBm | -82 dBm | -85 dBm |
| 5 GHz | -76 dBm | -78 dBm | -80 dBm |

**Note**

This feature is supported only on the following access points: AP-7522, AP 7532, AP 7562, AP-8432, AP-8533

6 In the Miscellaneous field, use the RIFS *(Reduced Interframe Spacing)* drop-down menu ro override interframe spacing settings.

| | |
|---|---|
| RIFS Mode | Interframe spacing is an interval between two consecutive Ethernet frames to enable a brief recovery between packets and allow target devices to prepare for the reception of the next packet.<br>Use this option to specify the interframe spacing settings:<br>• **`Receive Only`** - Select to apply interframe spacing only to packets received by this access point.<br>• **`Transmit Only`** - Select to apply interframe spacing only to packets transmitted by this access point.<br>• **`Transmit and Receive`** - Select to apply interframe spacing to packets both transmitted and received by this access point.<br>• **`None`** - Select to disable interframe spacing. Consider selecting this value for high priority traffic to reduce packet delay. |

7 Set or override the following Aeroscout Properties for the selected access point radio.

| | |
|---|---|
| Forward | Select this option to enable forwarding of Aeroscout packets. |
| MAC to be forwarded | Enter the MAC address that is incorporated in the Aeroscout packets that are forwarded. |

8 Set or override the following **Ekahau Properties** for the selected access point radio.

| | |
|---|---|
| Forwarding Host | Specify the IP address of the host to which Ekahau packets are forwarded. |
| Forwarding Port | Set the Ekahau forwarding port number. |
| MAC to be forwarded | Enter the MAC address that is incorporated in the Ekahau packets that are forwarded. |

9 Set or override the following **Non-Unicast Traffic** values for the profile's supported access point radio and its connected wireless clients:

| | |
|---|---|
| Non-Unicast Transmit Rate | Use the **Select** drop-down menu to launch a sub-screen to define the data rate for broadcast and multicast frame transmissions. If you are not using the same rate for each BSSID, seven different rates are available – each with a separate menu. |
| Non-Unicast Forwarding | Define whether client broadcast and multicast packets should always follow DTIM, or only follow DTIM when using Power Save Aware mode. The default setting is *Follow DTIM*. |

10 Refer to the **Sniffer Redirect (Packet Capture)** field to define or override the radio's captured packet configuration.

| | |
|---|---|
| Host for Redirected Packets | If packets are redirected from a controller or service platform's connected access point radio, specify the IP address of a resource (additional host system) used to capture the redirected packets. This address is the numerical (non DNS) address of the host used to capture the redirected packets. |
| Channel to Capture Packets | Specify the channel used to capture redirected packets. The default value is channel 1. |

11 Refer to the **Channel Scanning** field to define or override the radio's captured packet configuration.

| | |
|---|---|
| Enable Off-Channel Scan | Select to enable scan across all channels using this radio. Channel scans use access point resources and can be time consuming, so only enable when your sure the radio can afford the bandwidth be directed toward the channel scan and does not negatively impact client support. This option is disabled by default. |
| Off Channel Scan list for 5GHz | Select the list of channels for off-channel scans using the access point's 5GHz radio. Restricting off-channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 5GHz radio band. |
| Off Channel Scan list for 2.4GHz | Select the list of channels for off-channel scans using the access point's 2.4GHz radio. Restricting off-channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 2.4GHz radio band. |
| Max Multicast | Set the maximum number (from 0 - 100) of multicast/broadcast messages used to perform off-channel scanning. The default setting is 4. |
| Scan Interval | Set the interval (from 2 - 100 dtims) between off-channel scans. The default setting is 20 dtims. |
| Sniffer Redirect | Specify the IP address of the host to which captured off-channel scan packets are redirected. |

12 Click **OK** to save the changes and overrides to the **Advanced Settings** screen.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - PPPoE

PPPoE *(PPP over Ethernet)* is a data-link protocol for dialup connections. PPPoE allows the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables WiNG-supported controllers and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the access point's Wired WAN should fail.

Note

Devices with PPPoE enabled continue to support VPN, NAT, PBR, and 3G failover on the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

When PPPoE client operation is enabled, it discovers an available server and establishes a PPPoE link for traffic slow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, traffic is redirected back through the access point's wired WAN link.

When the access point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

Note

WiNG 7.1 releases does not provide PPPoE support on the AP505 and AP510 model access points. This feature will be supported in future releases.

To override an access point's PPPoE point-to-point interface configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Interface** and select **PPPoE**.

The existing PPPoE interface configuration is displayed.

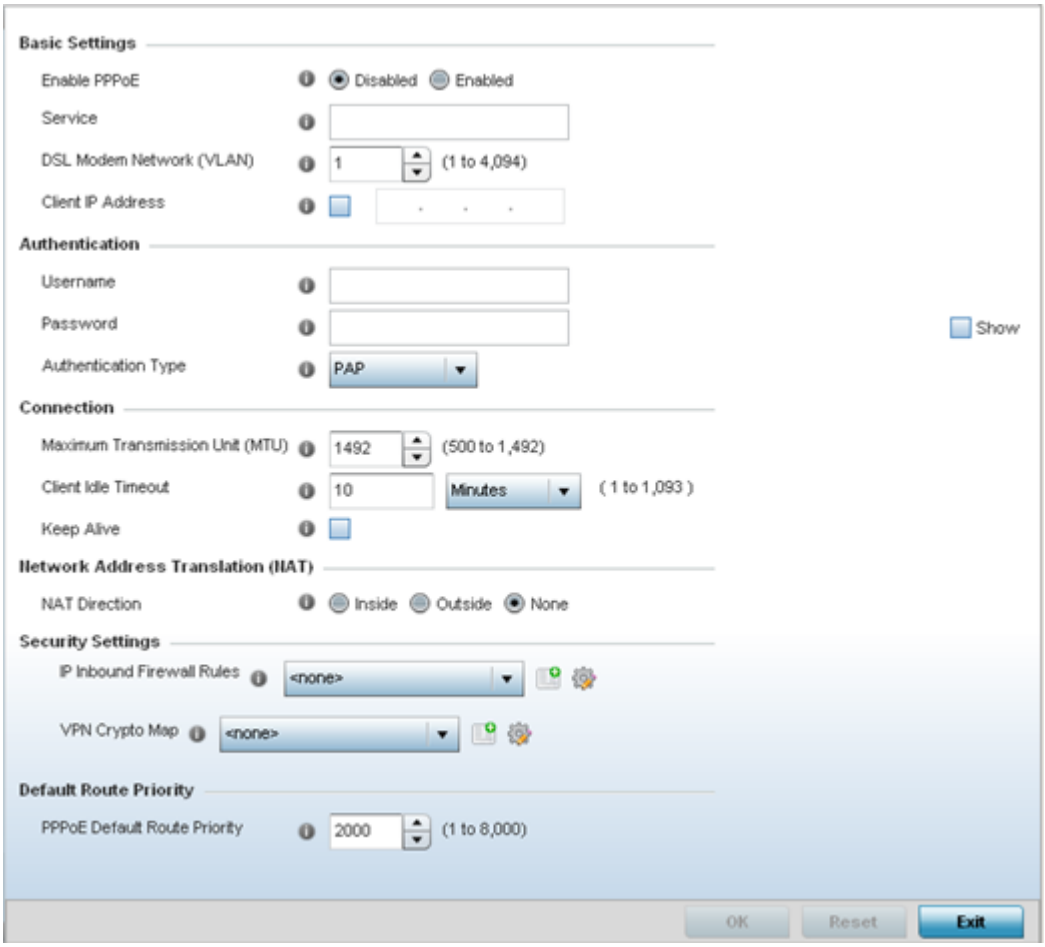



**Figure 169: Profile Overrides - PPPoE Interface Configuration Screen**

4 Use the Basic Settings field to enable PPPoE and define a PPPoE client.

| | |
|---|---|
| Service | Enter the 128-character maximum PPPoE client service name provided by the service provider. |
| DSL Modem Network (VLAN) | Set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to the DSL modem. The available range is 1 - 4,094. The default value is 1. |
| Client IP Address | Provide the numerical (non hostname) IP address of the PPPoE client. |

5 Define the following Authentication parameters for PPPoE client interoperation:

| | |
|---|---|
| Username | Provide the 64 character maximum username used for authentication support by the PPPoE client. |
| Password | Provide the 64 character maximum password used for authentication by the PPPoE client. Click **Show** to display the characters that make up the password. |
| Authentication Type | Specify the authentication type used by the PPPoE client, and whose credentials must be shared by its peer access point. Supported authentication options include **`None`**, **`PAP`**, **`CHAP`**, **`MSCHAP`**, and **`MSCHAP-v2`**. |

6 Define the following Connection settings for the PPPoE point-to-point connection with the PPPoE client:

| | |
|---|---|
| Maximum Transmission Unit (MTU) | Set the PPPoE client MTU *(maximum transmission unit)* from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492. |
| Client Idle Timeout | Set a timeout in either **`Seconds`** (1 - 65,535), **`Minutes`** (1 - 1,093) or **`Hours`** (1-18). The access point uses the defined timeout so it does not sit idle waiting for input from the PPPoE client and server that may never come. The default setting is 10 minutes. |
| Keep Alive | Select this option to ensure that the point-to-point connection to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default. |

7 Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

NAT converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point router maps its local (**`Inside`**) network addresses to WAN (**`Outside`**) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. The default setting is *None* (neither inside nor outside).

8 Define the following **Security Settings** for the PPPoE configuration:

| | |
|---|---|
| Inbound IP Firewall Rules | Select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If there is no firewall rule that meets the data protection needs of the PPPoE client connection, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing rule. For more information, see Wireless Firewall on page 730. |

9 Set the **Default Route Priority** for the default route learned using PPPoE.

Select from 1 - 8,000. The default setting is 2,000.

10 Click **OK** to save the changes and overrides made to the PPPoE screen.

Click **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

### Profile Overrides - Bluetooth

The AP7602, AP7612, AP7632, AP7662, AP8432 and AP8533 model access points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network.

These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

AP-8432 and AP-8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone- URL beacons. The access point's Bluetooth radio sends non-connectable, undirected LE *(low-energy)* advertisement packets on a periodic basis. These advertisement packets are short, and they are sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. Portions of the advertising packet are still customizable, however.

Note

WiNG 7.1 release does not support Bluetooth on AP505i and AP510i model acess points. This feature will be supported in future releases.

To override the access point's Bluetooth interface configuration:

1 Go to **Configuration → Devices → Device Overrides** .

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Interface** and select **Bluetooth**.

The access point's bluetooth interface configuration is displayed.

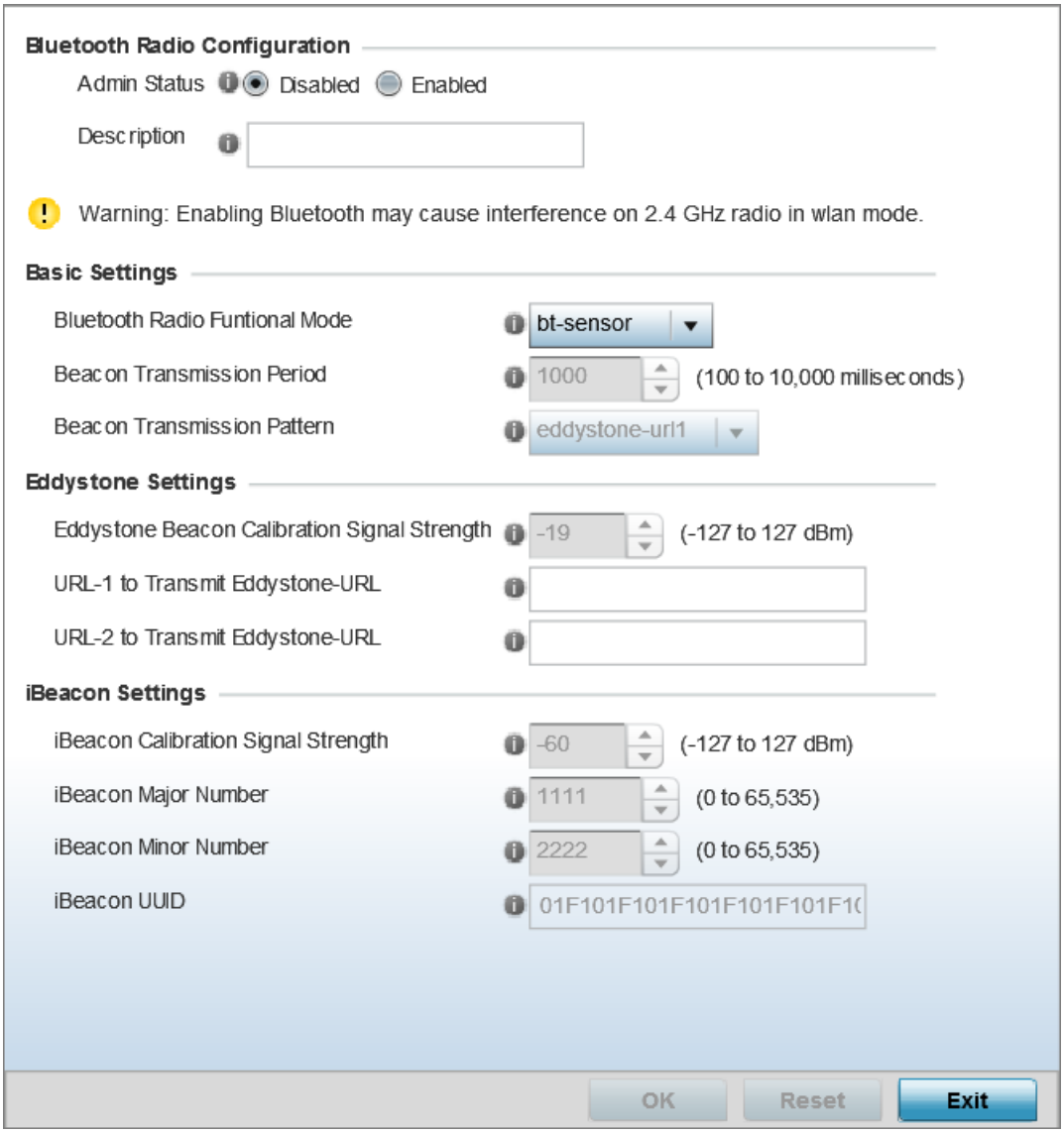



**Figure 170: Profile Overrides - Interface - Bluetooth Configuration Screen**

4 Set the following Bluetooth Radio Configuration parameters:

| | |
|---|---|
| Admin Status | Select **`Enabled`** or **`Disabled`** to enable/disable Bluetooth support capabilities for AP-8432 or AP-8533 model access point radio transmissions. The default value is *Disabled*. |
| Description | Define a 64 character maximum description for the access point's Bluetooth radio to differentiate this radio interface from other Bluetooth supported radio's that might be members of the same RF Domain. |

5 Set the following **Basic Settings**:

| | |
|---|---|
| Bluetooth Radio Functional Mode | Use this drop-down menu to set the access point's Bluetooth radio functional mode to one of the following options:<br>• **bt-sensor** - bt-sensors are Bluetooth classic sensors providing robust wireless connections for legacy devices. Typically these connections are not ideally suited for the newer Bluetooth low energy technology supported devices. This the default setting.<br>• **le-beacon** - le-beacons are newer Bluetooth low energy beacons ideal for applications requiring intermittent or periodic transfers of small amounts of data. le-beacons are not designed as replacements for classic beacon sensors.<br>Note:<br>Setting the Bluetooth Radio Functional mode to 'le-beacon' enables the '**Beacon Transmission Period**' and '**Beacon Transmission Pattern**' options.<br>• **le-tracking** - Sets the funtional mode to LE *(low energy)* tracking.<br>• **le-sensor** - Sets the funtional mode to LE sensor.<br>Note:<br>If enabling the *Bluetooth Radio Funtional Mode* as *le-beacon*, configure the 'Beacon Transmission Period' and 'Beacon Transmission Pattern' values. |
| Beacon Transmission Period | Use this spinner control to set the Bluetooth radio's beacon transmission period from 50 - 10,000 milliseconds. As the defined period increases, so does the CPU processing time and the number packets incrementally transmitted (typically one per minute). The default setting is 1,000 milliseconds.<br>Note:<br>This parameter is enabled when the functional mode is set to 'le-beacon'. |
| Beacon Transmission Pattern | Use this drop-down menu to set the beacon's transmission pattern. The options are:<br>• **eddystone_url1** and **eddystone_url2** - An eddystone-URL frame broadcasts a URL using a compressed encoding scheme to better fit within a limited advertisement packet. Once decoded, the URL can be used by a client for internet access.<br>• **ibeacon** - iBeacon was created by Apple for use in iOS devices (beginning with iOS version 7.0). Apple has made three data fields available to iOS applications: a UUID for device identification, a Major value for device class, and a Minor value for more refined information like product category.<br>Note:<br>This parameter is enabled when the functional mode is set to 'le-beacon'. |

6 If setting the Beacon Transmission Pattern to **eddystone_url1** or **eddystone_url2**, define the following Eddystone Settings settings:

| | |
|---|---|
| Eddystone Beacon Calibration Signal Strength | Set the Eddystone Beacon measured calibration signal strength, from -127 dBm to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters. The default setting is -19 dBm. |
| URL-1 to Transmit Eddystone-URL | Enter a 64-character maximum Eddystone-URL1. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a web server. |
| URL-2 to Transmit Eddystone-URL | Enter a 64-character maximum Eddystone-URL2. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a web server. |

7 If setting the Beacon Transmission Pattern to **ibeacon**, define the following iBeacon Settings :

| | |
|---|---|
| Beacon Calibration Signal Strength | Set the iBeacon measured calibration signal strength, from -127 dBm to 127 dBm, at 1 meter. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 1 meter. The default setting is -60 dBm. |
| iBeacon Major Number | Set the iBeacon major value from 0 - 65, 535. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. The default value is 1,111. |
| iBeacon Minor Number | Set the iBeacon minor value from 0 - 65, 535. Minor values identify and distinguish individual beacons. Minor values help identify individual beacons within a group of beacons assigned a major value. The default setting is 2,222. |
| iBeacon UUID | Define a 32 hex character maximum UUID *(Universally Unique IDentifier)*. The UUID classification contains 32 hexadecimal digits, split into 5 groups, separated by dashes – for example, `f2468da6-5fa8-2e84-1134- bc5b71e0893e`. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration. |

8 Select **OK** to save the changes to the Bluetooth configuration. Saved configurations are persistent across reloads.

Select **Reset** to revert to the last saved configuration.

### *Profile Overrides - Network*

Setting an acces point profile's network configuration is a large task comprised of numerous administration activities. Each of the activities described below can have an override applied to the original profile configuration. Applying an override removes the device from the profile configuration that may be shared by other devices and requires careful administration to ensure this one device still supports the deployment requirements within the managed network.

A profile's network configuration process consists of the following:



### Profile Overrides - DNS

DNS *(Domain Name System)* is a hierarchical naming system for resources connected to the Internet or a private network. Primarily, DNS resources translate domain names into IP addresses. If one DNS server doesn't know how to translate a particular domain name, it asks another one until the correct IP address is returned. DNS enables access to resources using human friendly notations. DNS converts human friendly domain names into notations used by different networking equipment for locating resources.

As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS, in the simplest terms, you would need to remember a series of numbers (123.123.123.123) instead of an easy to remember domain name (for example, *www.domainname.com*).

To override an access point's DNS configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network. Select a device.

2 Expand **Profile Overrides** → **Network** and select **DNS**.

The selected device's DNS configuration screen displays.

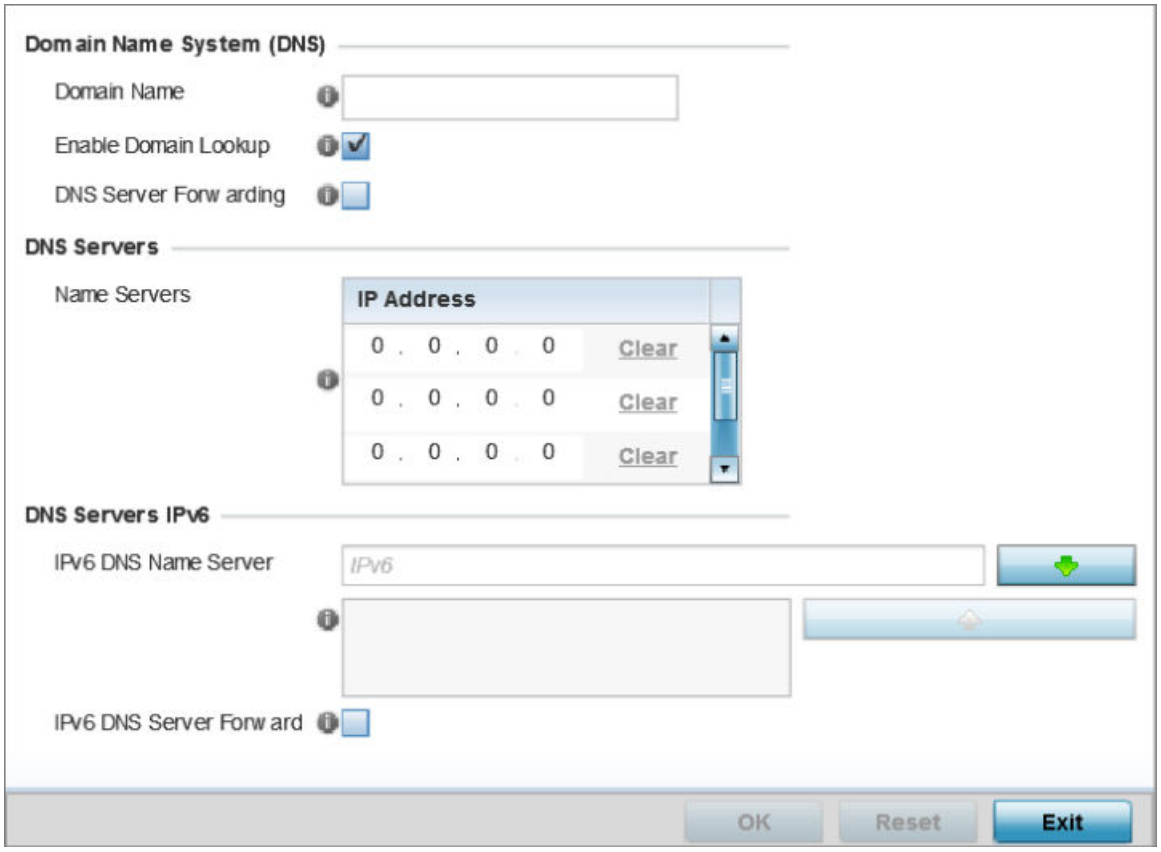



**Figure 171: Profile Overrides - Network DNS Configuration Screen**

3 In the Domain Name System (DNS) field set the following configurations:

| | |
|---|---|
| Domain Name | Provide the default Domain Name used to resolve DNS names. The name cannot exceed 64 characters. |
| Enable Domain Lookup | Select the check box to enable DNS. When enabled, human friendly domain names are converted into numerical IP destination addresses. The radio button is selected by default. |
| DNS Server Forwarding | Select this option to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by local DNS resources. This feature is disabled by default. |

4 In the DNS Servers field, provide the IP addresses of up to three Name Server resources available to the access point.

5 In the DNS Servers IPv6 field, set the following configurations:

| | |
|---|---|
| IPv6 DNS Name Server | Provide the default domain name used to resolve IPv6 DNS names. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted. |
| IPv6 DNS Server Forward | Select the check box to enable IPv6 DNS domain names to be converted into numerical IP destination addresses. The setting is disabled by default. |

6 Click **OK** to save the DNS configuration changes.
Click **Reset** to revert to the last saved configuration.

### Profile Overrides - ARP

ARP *(Address Resolution Protocol)* is a protocol for mapping an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, ARP is used to find a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to see if a device knows it has that IP address associated with it. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

To override the access point profile's ARP configuration:

1 Go to **Configuration** → **Devices** → **Device Overrides**.
The Device Overrides screen displays. This screen lists devices within the managed network.
2 Expand **Network** and select **ARP**.
The selected device's ARP configuration screen displays.

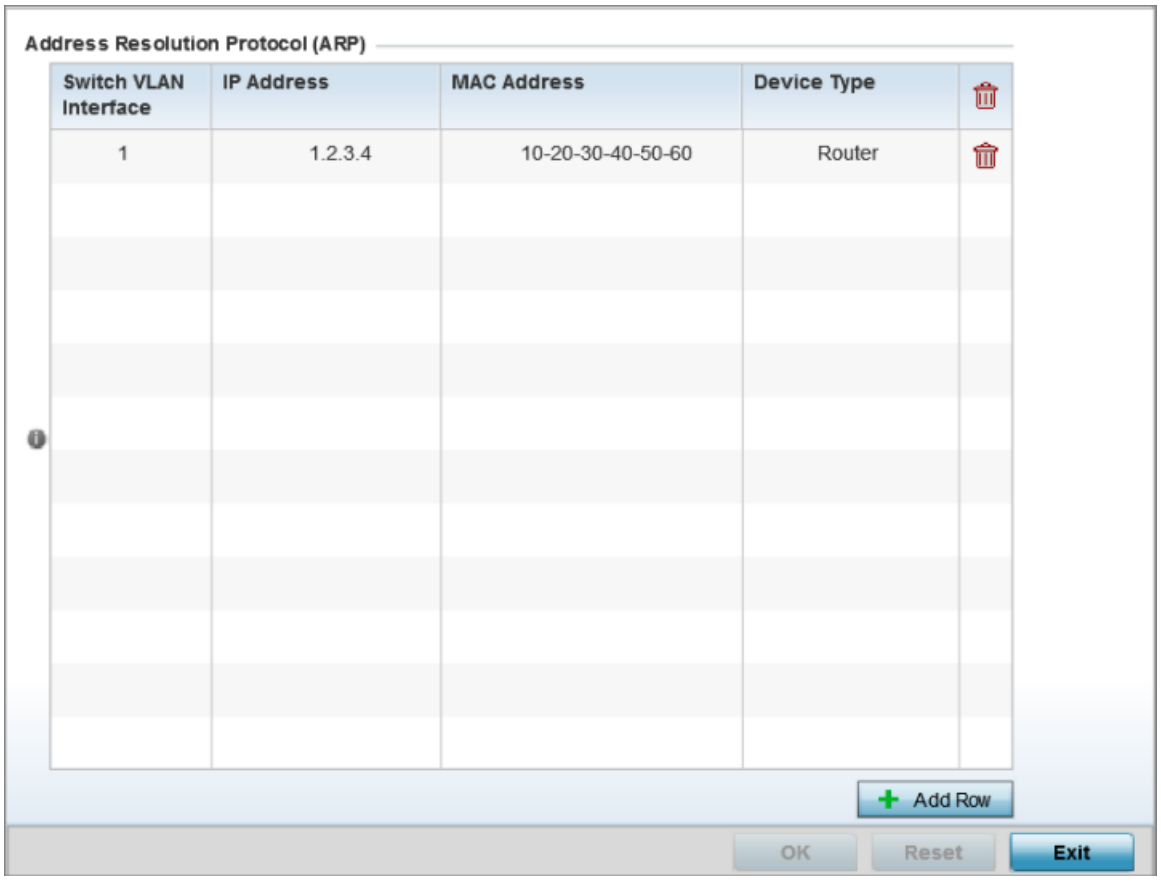



**Figure 172: Profile Overrides - Network - ARP Configuration Screen**

3 Select **+ Add Row** from the lower right-hand side of the screen to populate the ARP table with rows used to define ARP network address information.

4 Set the following the ARP parameters:

| | |
|---|---|
| Switch VLAN Interface | Use the spinner control to select a virtual interface for an address requiring resolution with the controller, service platform or access point. |
| IP Address | Define the IP address used to fetch a MAC Address recognized on the wireless network. |
| MAC Address | Displays the target MAC address subject to resolution. This is the MAC used for mapping an IP address to a MAC address recognized on the network. |
| Device Type | Specify the device type the ARP entry supports. Host is the default setting. |

5 Select **OK** to save the ARP configuration changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - L2TPv3 General Settings

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and profile). L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables controllers, service platforms and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WiNG managed devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. access points support an Ethernet VLAN pseudowire type exclusively.

Note

A pseudowire is an emulation of a layer 2 point-to-point connection over a PSN *(packet-switching network)* . A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-

alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

**Note**

If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

**Note**

WiNG 7.1 release does not support L2TPv3 tunneling on AAP505i and AP510i model access points. This feature will be supported in future releases.

To override the profile's L2TPv3 general configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select a target device by double-clicking on the device name.

The selected device's configuration menu displays.

3 Expand the **Network** node and select **L2TPv3**.

The L2TPv3 general configuration screen displays.

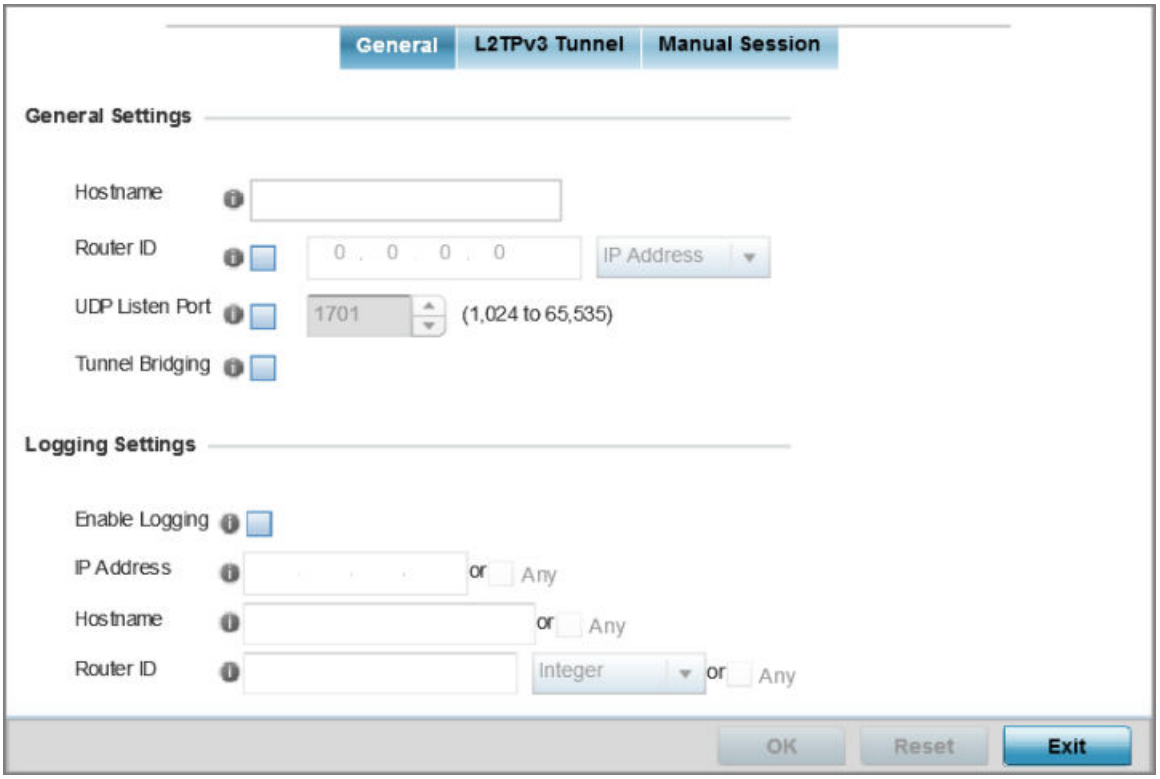



**Figure 173: L2TPv3 - General Configuration Screen**

4 Set the following General Settings for an L2TPv3 profile configuration:

| | |
|---|---|
| Host Name | Define a 64 character maximum hostname to specify the name of the host that's sent tunnel messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host. |
| Router ID | Set either the numeric IP address or the integer used as an identifier for tunnel AVP messages. AVP messages assist in the identification of a tunneled peer. |
| UDP Listen Port | Select this option to set the port used for listening to incoming traffic. Select a port from 1,024 - 65,535. The default port is 1701. |
| Tunnel Bridging | Select this option to enable or disable bridge packets between two tunnel end points. This setting is disabled by default. |

5 Set the following Logging Settings for a L2TPv3 profile configuration:

| | |
|---|---|
| Enable Logging | Select this option to enable the logging of Ethernet frame events to and from bridge VLANs and physical ports on a defined IP address, host or router ID. This setting is disabled by default. |
| IP Address | Optionally use a peer tunnel ID address to capture and log L2TPv3 events. |
| Hostname | If not using an IP address for event logging, optionally use a peer tunnel hostname to capture and log L2TPv3 events. |
| Router ID | If not using an IP address or a hostname for event logging, use a router ID to capture and log L2TPv3 events. |

6 Click **OK** to save the L2TPv3 general configuration changes.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - L2TPv3 Tunnel

To override a profile's L2TPv3 tunnel configuration at the device level:

1 Select the **L2TPv3 Tunnel** tab.

The L2TPv3 main screen displays. This screen lists existing L2TPv3 tunnel configurations.

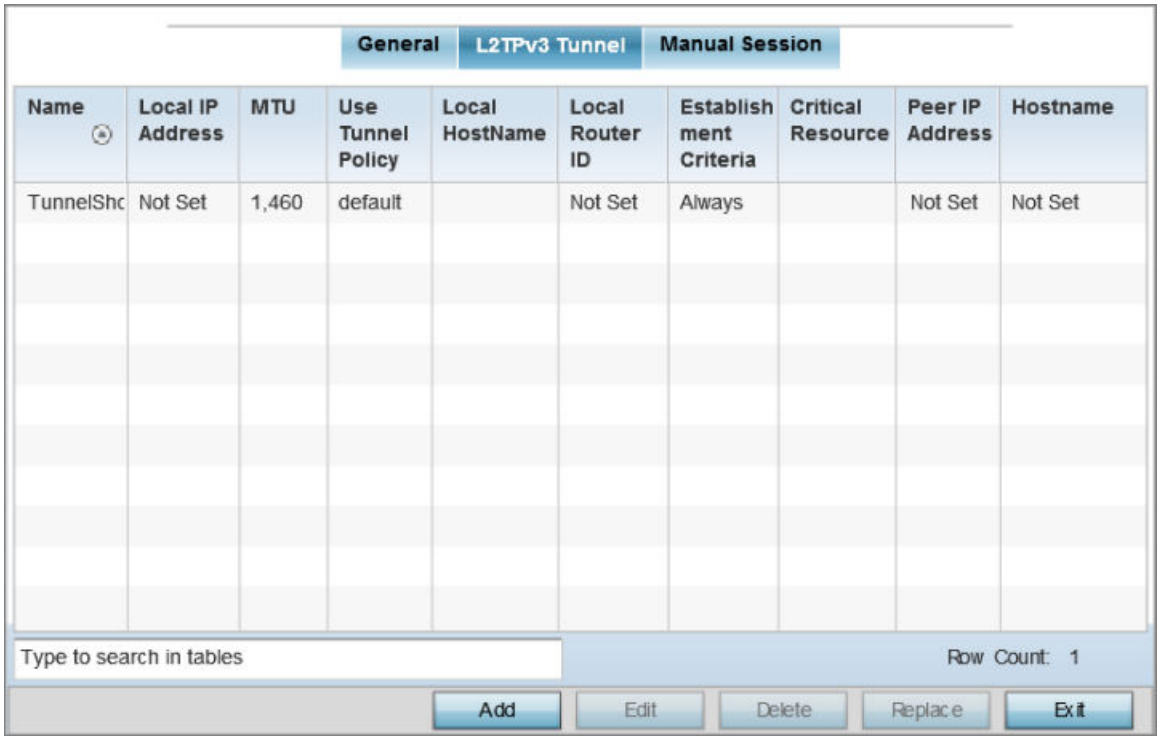



**Figure 174: L2TPv3 Tunnel Main Screen**

2 Review the following L2TPv3 Tunnel configuration data:

| | |
|---|---|
| Name | Displays the name of each listed L2TPv3 tunnel assigned upon creation. |
| Local IP Address | Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. |
| MTU | Displays the MTU size for each listed tunnel. The MTU is the size (in bytes) of the largest protocol data unit that the layer can pass between tunnel peers. |
| Use Tunnel Policy | Lists the L2TPv3 tunnel policy assigned to each listed tunnel. |
| Local Hostname | Lists the tunnel specific hostname used by each listed tunnel. This is the hostname advertised in tunnel establishment messages. |
| Local Router ID | Specifies the router ID sent in the tunnel establishment messages. |
| Establishment Criteria | Specifies tunnel criteria between two peers. |
| Critical Resource | Specifies the critical resource that should exist for a tunnel between two peers to be created and maintained. Critical resources are device IP addresses or interface destinations interpreted as critical to the health of the network. The critical resource feature allows for the continuous monitoring of these defined addresses. A critical resource, if not available, can result in the network suffering performance degradation. |

| | |
|---|---|
| Peer IP Address | Lists the IP address of the remote peer. |
| Host Name | Lists the tunnel specific hostname used by the remote peer. |

Session Configuration

You can add a new L2TPv3 tunnel configuration or eidt an existing configuration.

1 Click **Add** to create a new L2TPv3 tunnel. If creating a new tunnel configuration, assign it a 31 character maximum `Name`.

2 To override the profile's L2TPv3 tunnel configuration, select the L2TPv3 tunnel from those listed on the screen and click **Edit**.

The L2TPv3 tunnel configuration screen displays, with the Session tab selected by default.

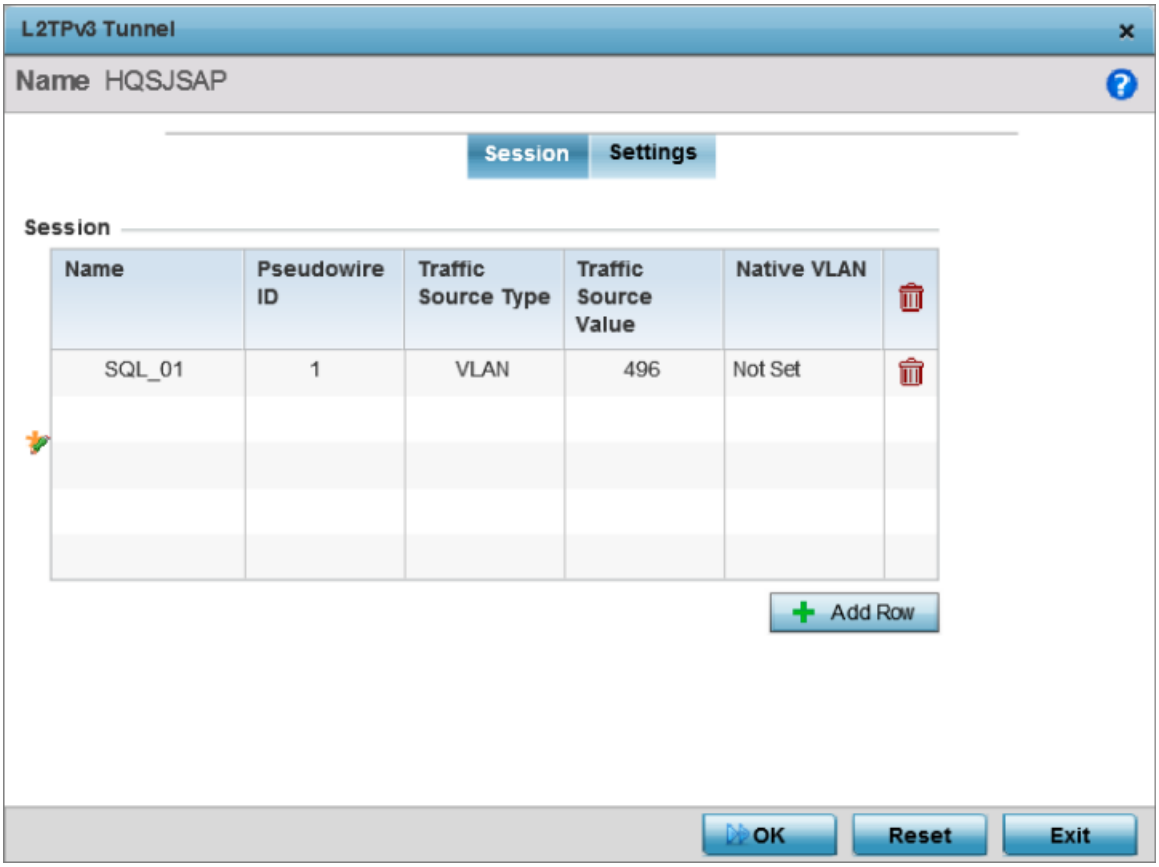



**Figure 175: L2TPv3 Tunnel - Session Configuration Screen**

3 Refer to the Session table to review the configurations of the peers available for tunnel connection.

4 Select **+ Add Row** and provide the following L2TPv3 session settings:

| | |
|---|---|
| Name | Enter a 31 character maximum session name. There is no idle timeout for a tunnel. A tunnel is not usable without a session and a subsequent session name. The tunnel is closed when the last session tunnel session is closed. |
| Pseudowire ID | Define a psuedowire ID for this session. A pseudowire is an emulation of a layer 2 point-to-point connection over a PSN. A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network. |
| Traffic Source Type | Lists the type of traffic tunneled in this session (VLAN, etc.). |
| Traffic Source Value | Define a VLAN range to include in the tunnel session. Available VLAN ranges are from 1 - 4,094. |
| Native VLAN | Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer. |

5 Click **OK** to save the L2TPv3 Tunnel session changes.

Settings Configuration

To define or override the L2TPv3 tunnel settings:

1 Select the **Settings** tab.

The L2TPv3 Tunnel Settings configuration screen displays.

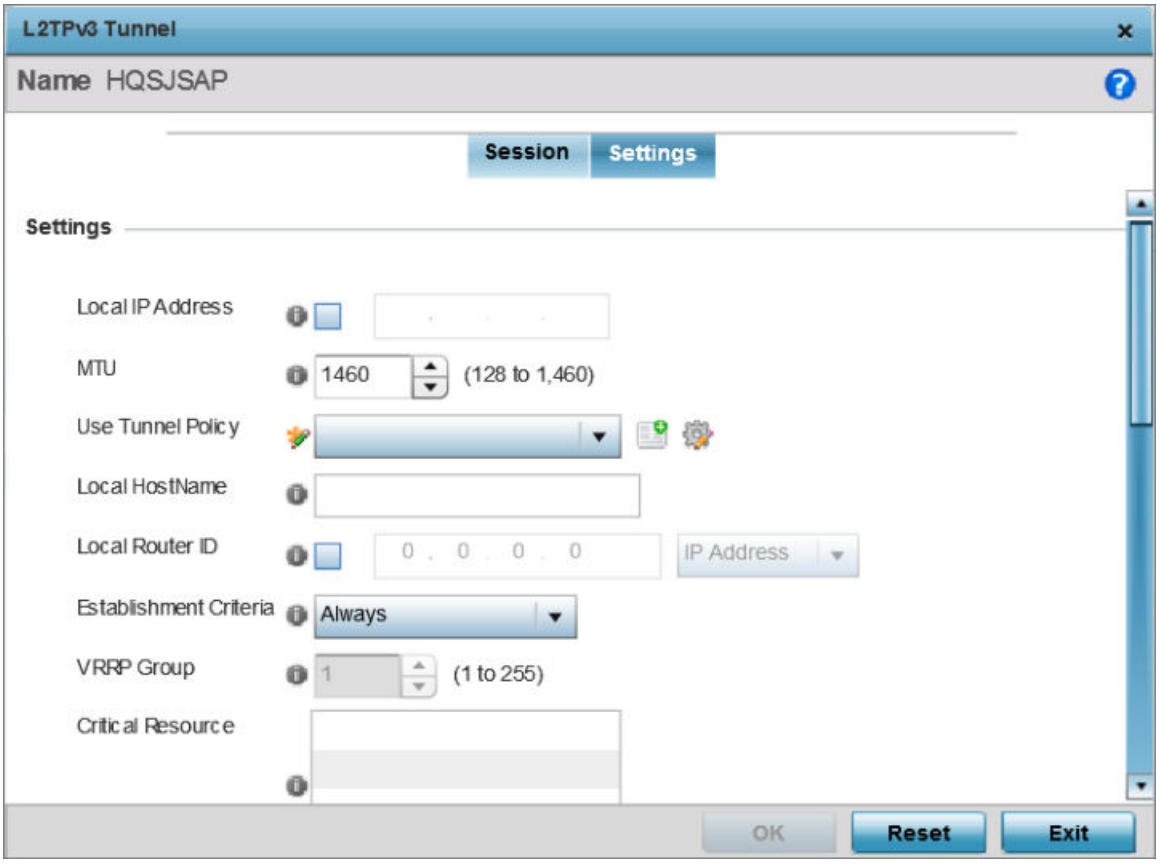



**Figure 176: L2TPv3 Tunnel - Settings Configuration Screen**

2 Define the following L2TP v3 Tunnel **Settings**:

| | |
|---|---|
| Local IP Address | Enter the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the tunnel and responding to incoming tunnel create requests. |
| MTU | Set the MTU. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers. Define a MTU between 128 - 1,460 bytes. The default setting is 1,460. A larger MTU means processing fewer packets for the same amount of data. |
| Use Tunnel Policy | Select the L2TPv3 tunnel policy. The policy consists of user defined values for protocol specific parameters which can be used with different tunnels. If none is available a new policy can be created or an existing one can be modified. For more information, refer to L2TP V3 Configuration on page 681. |
| Local Hostname | Provide the tunnel specific hostname used by this tunnel. This is the hostname advertised in tunnel establishment messages. |
| Local Router ID | Specify the router ID sent in tunnel establishment messages with a potential peer device. |
| Establishment Criteria | Configure establishment criteria for creating a tunnel between the device and the NOC. This criteria ensures only one tunnel is created between two sites where the tunnel is established between the vrrp-master/cluster master/ rfdomain manager at the remote site and the controller at the NOC. The tunnel is created based on the role of the remote peer.<br>• **`always`** – The tunnel is always created irrespective of the role of the local device.<br>• **`vrrp-master`** – The tunnel is only created when the local device is a VRRP master.<br>• **`cluster-master`** – The tunnel is only created when the local device is a cluster master.<br>• **`rf-domain-manager`** – The tunnel is only created when the local device is a RF-Domain manager.<br>In all the above cases, if the local device goes offline for any reason, the tunnel is brought down. |
| VRRP Group | This field is enabled only when the *establishment criteria* is set to *vrrp-master*. Use the spinner to select the VRRP group. |
| Critical Resource | Enter the critical resources required for creating and maintaining a L2TPV3 tunnel. A tunnel is only established when all critical resources for the tunnel to be operational are available at the time when the tunnel is created. If any one of the listed critical resources goes down, the tunnel is disabled. When a tunnel is established, the listed critical resources are checked for availability. Tunnel establishment is started if the critical resources are available. Similarly, for incoming tunnel termination requests, listed critical resources are checked and tunnel terminations are only allowed when the critical resources are available. For more information on managing critical resources, see Profile Overrides - List of Critical Resources on page 500 . |

3 Define the following **Rate Limit** settings:

Rate limiting manages the maximum rate sent to or received from L2TPv3 tunnel members.

| | |
|---|---|
| Session Name | Use the drop-down menu to select the tunnel session that will have the direction, burst size and traffic rate settings applied. |
| Direction | Select the direction for L2TPv3 tunnel traffic rate limiting. Egress traffic is outbound L2TPv3 tunnel data coming to the controller, service platform or access point. Ingress traffic is inbound L2TPv3 tunnel data coming to the controller, service platform or access point. |
| Max Burst Size | Set the maximum burst size for egress or ingress traffic rate limiting (depending on which direction is selected) on a L2TPv3 tunnel. Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for L2TPv3 tunnel traffic. The default setting is 320 bytes. |
| Rate | Set the data rate (from 50 - 1,000,000 kbps) for egress or ingress traffic rate limiting (depending on which direction is selected) for an L2TPv3 tunnel. The default setting is 5000 kbps. |
| Background | Set the random early detection threshold in % for background traffic. Set a value from 1 - 100%. The default is 50%. |
| Best-Effort | Set the random early detection threshold in % for best-effort traffic. Set a value from 1 - 100%. The default is 50%. |
| Video | Set the random early detection threshold in % for video traffic. Set a value from 1 - 100%. The default is 25%. |
| Voice | Set the random early detection threshold in % for voice traffic. Set a value from 1 - 100%. The default is 25%. |

4 Review the **Peer** configurations. Select **+ Add Row** and configure a maximum of two peer configurations.

5 Define the following **Peer** parameters:

| | |
|---|---|
| Peer ID | Define the primary peer ID used to set the primary and secondary peer for tunnel fail over. If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this access point, it creates the tunnel if the hostname and/or Router ID matches. |
| Router ID | Specify the router ID sent in tunnel establishment messages with this specific peer. |
| Hostname | Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process. |
| Encapsulation | Select either **IP** or **UDP** as the peer encapsulation protocol. UDP uses a simple transmission model without implicit handshakes. The default setting is *IP*. |
| Peer IP Address | Select this option to enter the numeric IP address used as the destination peer address for tunnel establishment. |
| UDP Port | If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. |
| IPSec Secure | Enable this option to enable security on the connection between the access point and the Virtual Controller. |
| IPSec Gateway | Specify the IP Address of the IPSec Secure Gateway. |

6 Define the following Fast Failover parameters:

| | |
|---|---|
| Enable | When enabled, the device starts sending tunnel requests on both peers, and in turn, establishes the tunnel on both peers. If disabled, tunnel establishment only occurs on one peer, with failover and other functionality the same as legacy behavior. If fast failover is enabled after establishing a single tunnel the establishment is restarted with two peers. One tunnel is defined as active and the other as standby. Both tunnels perform connection health checkups with individual hello intervals. This setting is disabled by default. |
| Enable Aggressive Mode | When enabled, tunnel initiation hello requests are set to zero. For failure detections, hello attempts are not retried, regardless of defined retry attempts. This setting is disabled by default. |

7 Click **OK** to save the L2TPv3 Tunnel changes.

Click **Reset** to revert the screen to its last saved configuration.

Profile Overrides - Manual Session

After successful tunnel connection and establishment, you can create individual sessions. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

To override a profile's L2TPv3 manual session configuration at the device level:

1 Select the **Manual Session** tab.

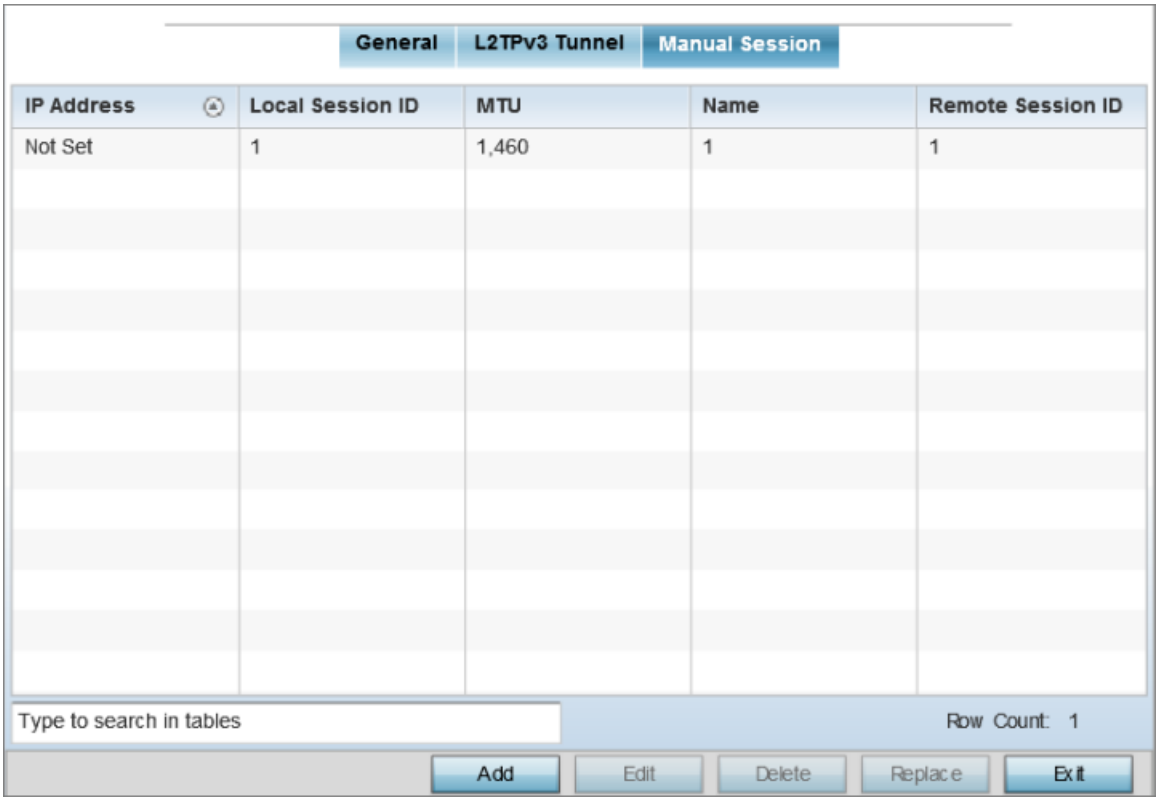



**Figure 177: L2TPv3 Tunnel - Manual Session Configuration Screen**

2 Review the existing manual session configurations, to determine whether a session should be created or modified:

| | |
|---|---|
| IP Address | Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the session and responding to incoming requests. |
| Local Session ID | Displays the numeric identifier assigned to each listed tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer. |
| MTU | Displays each session's MTU. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data. |
| Name | Lists the name assigned to each listed manual session. |
| Remote Session ID | Lists the remote session ID passed in the establishment of the tunnel, used a unique identifier for this tunnel session. |

Adding and Editing Manual Session

You can add a new L2TPv3 manual session configuration or edit an existing configuration.

1 Click **Add** to create a new L2TPv3 manual session. If creating a new configuration, assign it a 31 character maximum `Name`.

After a successful tunnel connection and establishment, the session is created. Each session name represents a single data stream.

2 To override the profile's L2TPv3 manual session configuration, select the L2TPv3 session from those listed on the screen and click **Edit**.

The L2TPv3 manual session configuration screen displays.

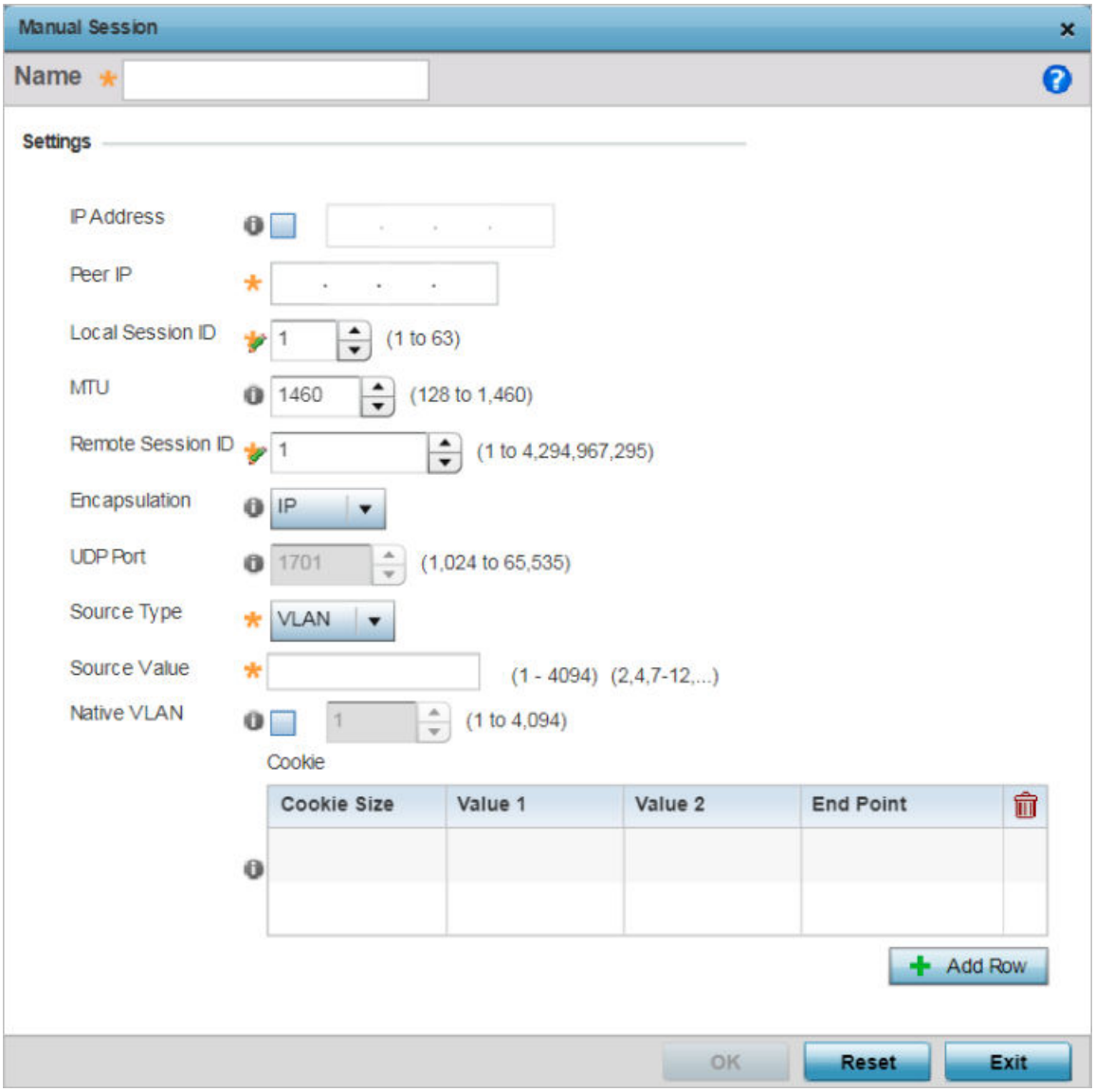



**Figure 178: L2TPv3 - Manual Session Configuration Screen**

3 Set or override the following session parameters:

| | |
|---|---|
| IP Address | Specify the IP address used to be as tunnel source IP address. If not specified, the tunnel source IP address is selected automatically based on the tunnel peer IP address. This address is applicable only for initiating the tunnel. When responding to incoming tunnel create requests, it would use the IP address on which it had received the tunnel create request. |
| Peer IP | Set the IP address of an L2TP tunnel destination peer. This is the peer allowed to establish the tunnel. |

| | |
|---|---|
| Local Session ID | Set the numeric identifier for the tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer. |
| MTU | Define the session's MTU *(maximum transmission unit)* as the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data. |
| Remote Session ID | Use the spinner control to set the remote session ID passed in the establishment of the tunnel and set a unique identifier for this tunnel session. Assign an ID from 1 - 4,294,967,295. |
| Encapsulation | Select either IP or UDP as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes. |
| UDP Port | If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. This is the port where the L2TP service is running. |
| Source Type | Select a VLAN as the virtual interface source type. |
| Source Value | Define the Source Value range (1 - 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames. |
| Native VLAN | Select this option to define the native VLAN that's not tagged. |

4 Select the **+ Add Row** button, in the Cookie table, to set the following:

| | |
|---|---|
| Cookie Size | Set the size of the cookie field within each L2TP data packet. Options include **0**, **4** and **8**. The default setting is 0. |
| Value 1 | Set the cookie value first word. |
| Value 2 | Set the cookie value second word. |
| End Point | Define whether the tunnel end point is **`local`** or **`remote`**. |

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

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - GRE

GRE *(Generic routing encapsulation)* tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over a GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, access points map one or more VLANs to a tunnel. The remote endpoint is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. access points can reach both the GRE peer as well as the RADIUS server using IPv4.

To override an access point's GRE tunnel configuration.

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Network** and select **GRE**.

The GRE Tunnel screen displays. This screen lists existing GRE tunnel configurations.

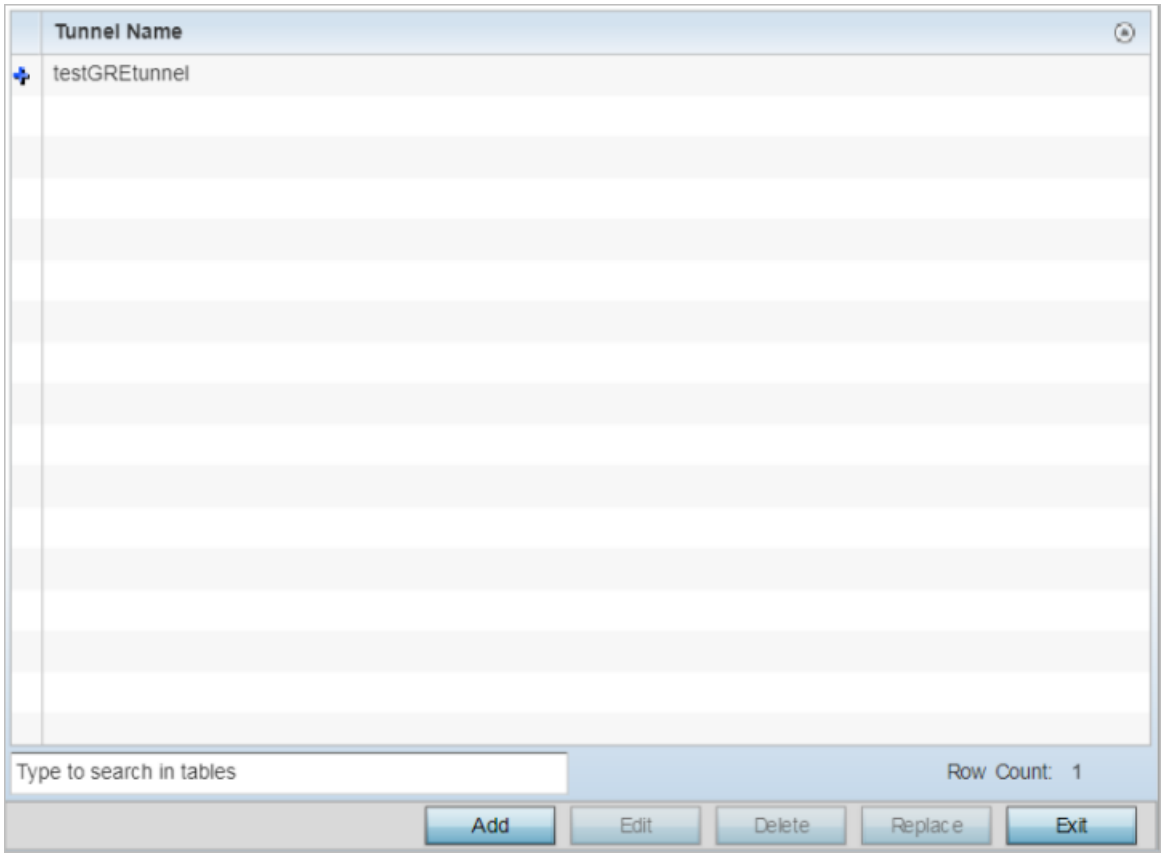



**Figure 179: Profile Overrides - Network - GRE Configuration Main Screen**

4 Select a tunnel from those listed on the screen and click **Edit**.

You can add new tunnels or delete existing tunnels.

The GRE tunnel configuration screen displays.

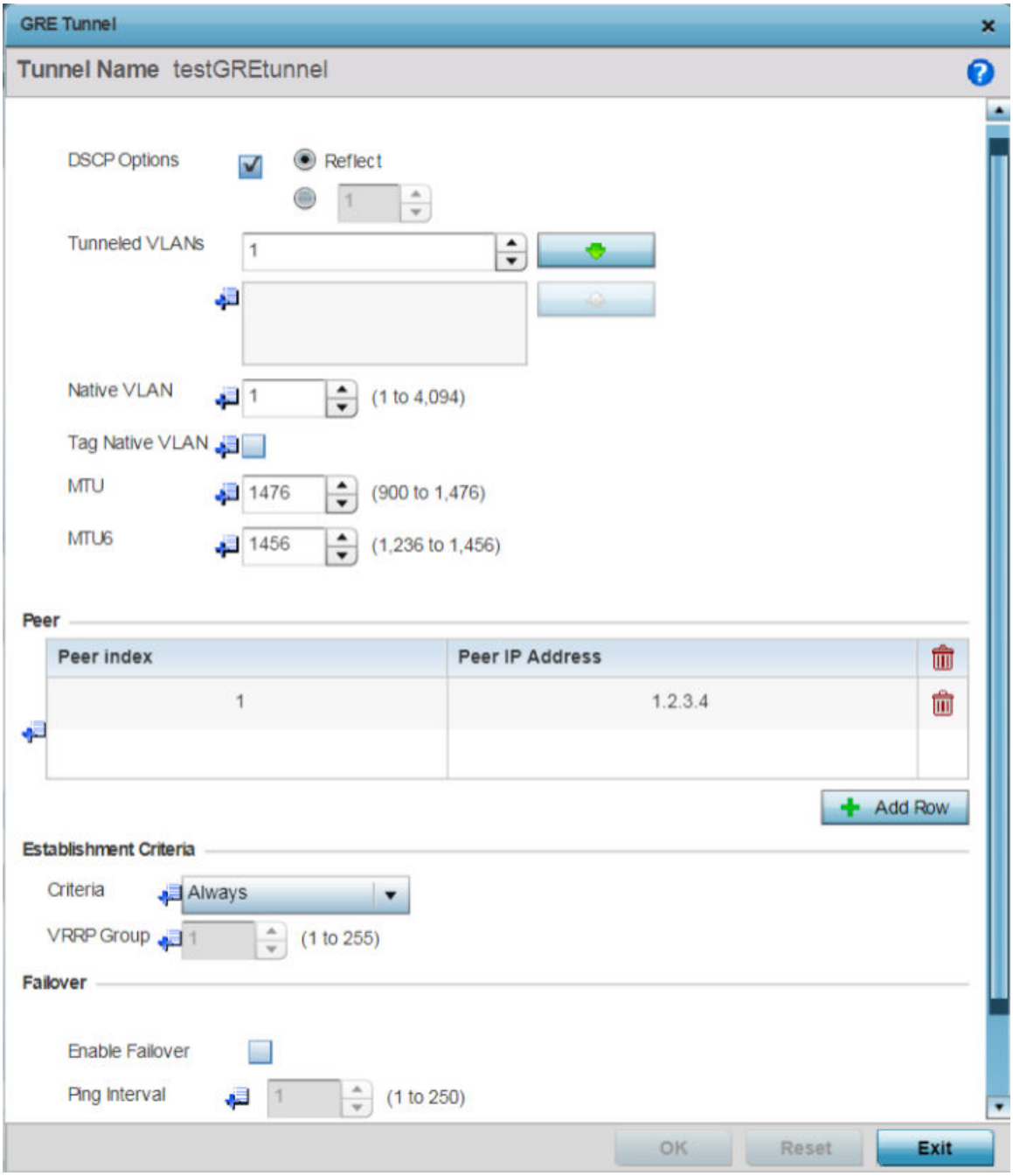



**Figure 180: GRE Tunnel - Add/Edit Configuration Screen**

5 If creating a new GRE tunnel, assign it a name to distinguish its configuration.

6 Define the following GRE tunnel configurations:

| | |
|---|---|
| DSCP Options | Use the spinner control to set the tunnel DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header. |
| Tunneled VLANs | Define the VLAN connected clients use to route GRE tunneled traffic within their respective WLANs. |
| Native VLAN | Set a numerical VLAN ID (1 - 4094) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode. |
| Tag Native VLAN | Select this option to tag the native VLAN. The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default. |

7 In the **Peer** table, click **+Add Row** and provide a maximum of two peer configurations.

The *Peer* table lists the credentials of the GRE tunnel end points.

| | |
|---|---|
| Peer Index | Assign a numeric index to each peer to help differentiate tunnel end points. |
| Peer IP Address | Define the IP address of the added GRE peer to serve as a network address identifier. |

8 Set the following **Establishment Criteria** for the GRE tunnel:

| | |
|---|---|
| Criteria | Specify the establishment criteria for creating a GRE tunnel. In a multicontroller within a RF domain, it's always the master node with which the tunnel is established. Dependimg on which of the following options is selected, the GRE is established:<br>• **`vrrp-master`** - The tunnel is created only if the master node is the VRRP master.<br>• **`cluster-master`** - The tunnel is created only if the master node is the cluster master.<br>• **`rf-domain-manager`** - The tunnel is created only if the master node is the RF Domain manager.<br>• **`always`** - The tunnel is automatically created, irrespective of whether the master node (device) is any one of the above three (3). In other words, the master node need not be any of the above three for the tunnel to be established. |
| VRRP Group | Set the VRRP group ID only enabled when the *Establishment Criteria* is set to *vrrp-master*. A virtual router redundancy group nables the creation of a group of routers as a default gateway for redundancy. Clients can point to the IP address of the VRRP virtual router as their default gateway and utilize a different group member if a master becomes unavailable. |

9 Define the following Failover parameters:

| | |
|---|---|
| Enable Failover | Select this option to periodically ping the primary gateway to assess its availability for failover support. |
| Ping Interval | Set the duration between two successive pings to the gateway. Define this value in seconds from 0 - 86,400. |
| Number of Retries | Set the number of retry ping opportunities before the session is terminated. |

10 Select the **OK** button located to save the changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - IGMP Snooping

The IGMP *(Internet Group Management Protocol)* is used for managing IP multicast group members. Controllers and service platforms listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the controller or service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

To override the access point's IGMP snooping configuration,

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Network** and select **IGMP Snooping**.

The IGMP Snooping configuration screen displays.

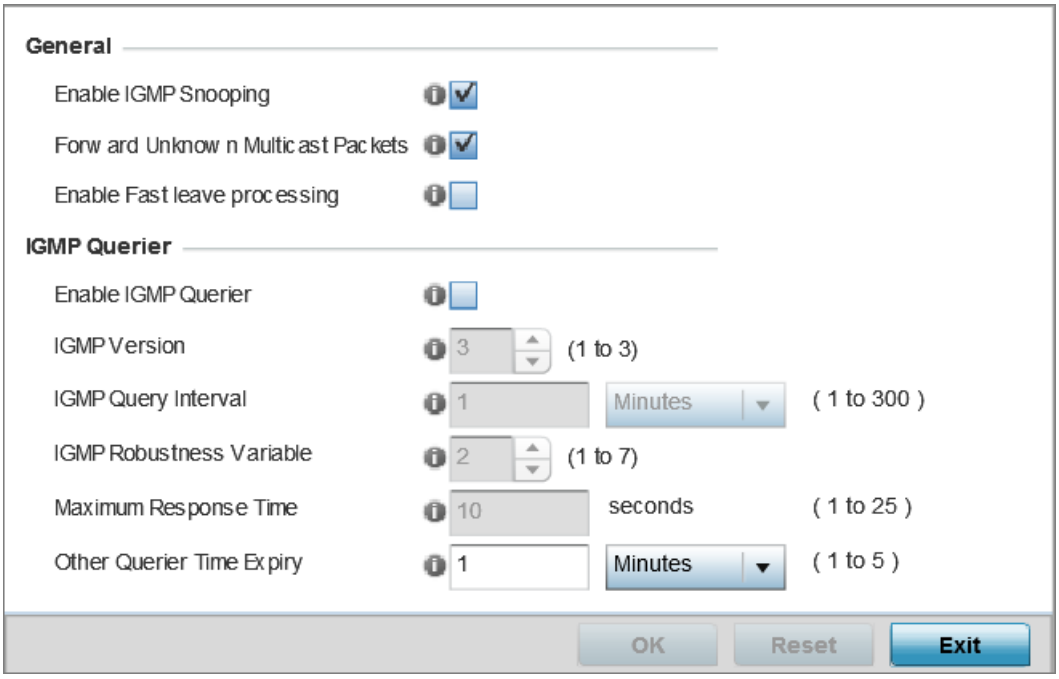



**Figure 181: Profile Overrides - Network - IGMP Snooping Configuration Screen**

4 Set the following General IGMP Snooping parameters:

| | |
|---|---|
| Enable IGMP Snooping | Select this option to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under the bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the effective setting is disabled. |
| Forward Unknown Multicast Packets | Select this option to enable the forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This setting is enabled by default. |

5 Set the following for **IGMP Querier** configuration:

| | |
|---|---|
| Enable IGMP Querier | Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server and hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port. |
| IGMP Version | Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 defined by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 by adding the ability to listen to multicast traffic originating from a set of source IP addresses exclusively. The default setting is 3. |
| IGMP Query Interval | Set the interval IGMP queries are made. This parameter is used only when the querier functionality is enabled. Define an interval value in **Seconds** (1 - 18,000), **Minutes** (1 - 300) and **Hours** (1 - 5). The default setting is one minute. |
| IGMP Robustness Variable | Sets the IGMP robustness variable. The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. Define a robustness variable from 1 - 7. The default robustness value is 2. |
| Maximum Response Time | Specify the maximum interval (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. Only multicast packets are forwarded to radios present in the snooping table. For IGMP reports from wired ports, the controller or service platform forwards these reports to the multicast router ports. The default setting is 10 seconds. |
| Other Querier Timer Expiry | Specify an interval in either **Seconds** (60 - 300) or **Minutes** (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute. |

6 Select **OK** to save the IGMP snooping configuration changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - MLD Snooping

MLD *(Multicast Listener Discovery)* snooping enables a controller, service platform or access point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to

discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or access point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To override the access point's MLD snooping configuration,

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Network** and select **MLD Snooping**.

The MLD Snooping configuration screen displays.

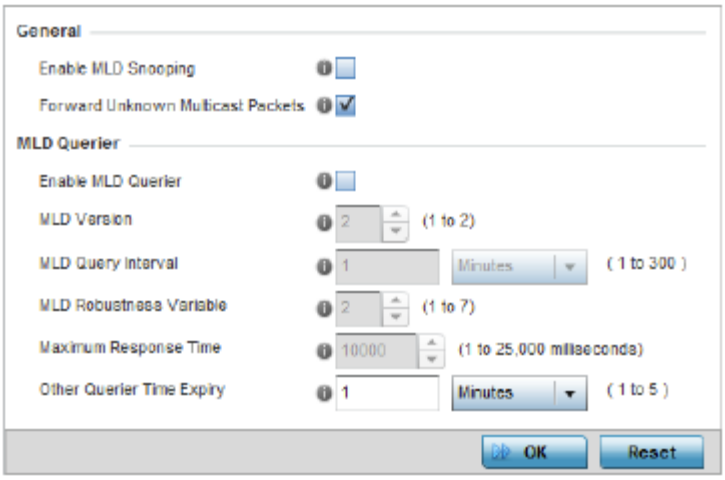



**Figure 182: Profile Overrides - Network - MLD SNooping Confgiuration Screen**

4 Define the following General settings:

| | |
|---|---|
| Enable MLD Snooping | Enable MLD snooping to examine MLD packets and make content forwarding for this profile. Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast. MLD snooping is disabled by default. |
| Forward Unknown Multicast Packets | Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default. |

5 Define the following MLD Querier settings:

| | |
|---|---|
| Enable MLD Querier | Select this option to enable MLD querier on the controller, service platform or access point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is disabled by default. |
| MLD Version | Define whether MLD version 1 or 2 is utilized as the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2. |
| MLD Query Interval | Set the interval in which query messages are sent to discover device multicast group memberships. Set an interval in either Seconds (1 -18,000), Minutes (1 - 300) or Hours (1 - 5). The default interval is 1 minute. |
| MLD Robustness Variable | Set a MLD IGMP robustness value (1 - 7) used by the sender of a query. The MLD robustness variable enables refinements to account for expected packet loss on a subnet. Increasing the robust count allows for more packet loss, but increases the leave latency of the subnetwork unless the value is zero. The default variable is 2. |
| Maximum Response Time | Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 10 milliseconds. |
| Other Querier time Expiry | Specify an interval in either Seconds (60 - 300) or Minutes (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute. |

6 Select **OK** to save the MLD Snooping configuration changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - Quality of Service (QoS)

The WiNG software uses different *Quality of Service* (QoS) screens to define WLAN and device radio QoS configurations.

QoS values are required to provide service priority to packets. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

The profile QoS screen maps the 6-bit Differentiated Service Code Point (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies a specific per-hop behavior that is applied to a packet. This QoS assignment can be overridden as needed, but removes the device configuration from the profile that may be shared with other similar access point models.

To override an access point profile's QoS configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **Quality of Service (QoS)**.

The **Traffic Shaping** → **Basic Configuration** screen displays by default.

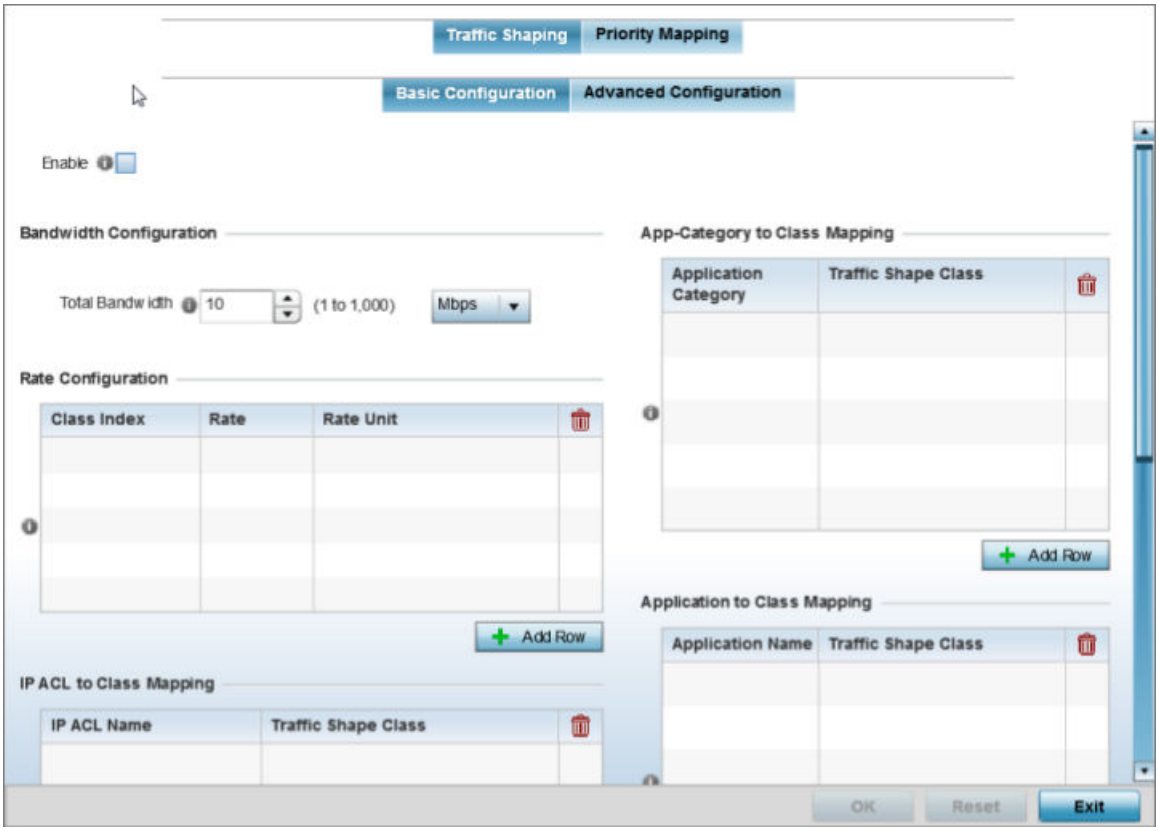



**Figure 183: QoS - Traffic Shaping - Basic Configuration Screen**

4 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, applications have priority, followed by application categories, then ACLs.

5 Set the **Total Bandwidth** configurable for the traffic shaper. Set the value from either 1 - 1,000 Mbps, or from 250 - 1,000,000 Kbps.

6 Select **+ Add Row** within the Rate Configuration table to set the Class Index (1 - 4) and Rate (in either Kbps, Mbps or percentage) for the traffic shaper class. Use the rate configuration to control the maximum traffic rate sent or received on the device. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.

7 Refer to the IP ACL Class Mapping table and select **+ Add Row** to apply an IPv4 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings.

8 Refer to the IPv6 ACL Class Mapping table and select **+ Add Row** to apply an IPv6 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings.

Note

For more information on creating IP based firewall rules, refer to Configuring IP Firewall Rules on page 744 and Setting an IPv4 or IPv6 Firewall Policy on page 745.

9 Refer to the **App-Category to Class Mapping** table and select + Add Row to apply an application category to shaper class mapping. Select + Add Row to add mappings by selecting the application category and its traffic shaper class. For more information on creating an application category, refer to Application on page 718.

10 Refer to the **Application to Class Mapping** table and select + Add Row to apply an application to shaper class mapping. Select **+ Add Row** to add mappings by selecting the application and its traffic shaper class. For more information on creating an application, refer to Application on page 718.

11 Select the **OK** button to save the traffic shaping basic configuration changes.

Select **Reset** to revert to the last saved configuration.

Profile Overrides - Advanced Traffic Shaping

1 Select the **Traffic Shaping → Advanced Configuration** tab.

The **Traffic Shaping → Advanced Configuration** screen displays.

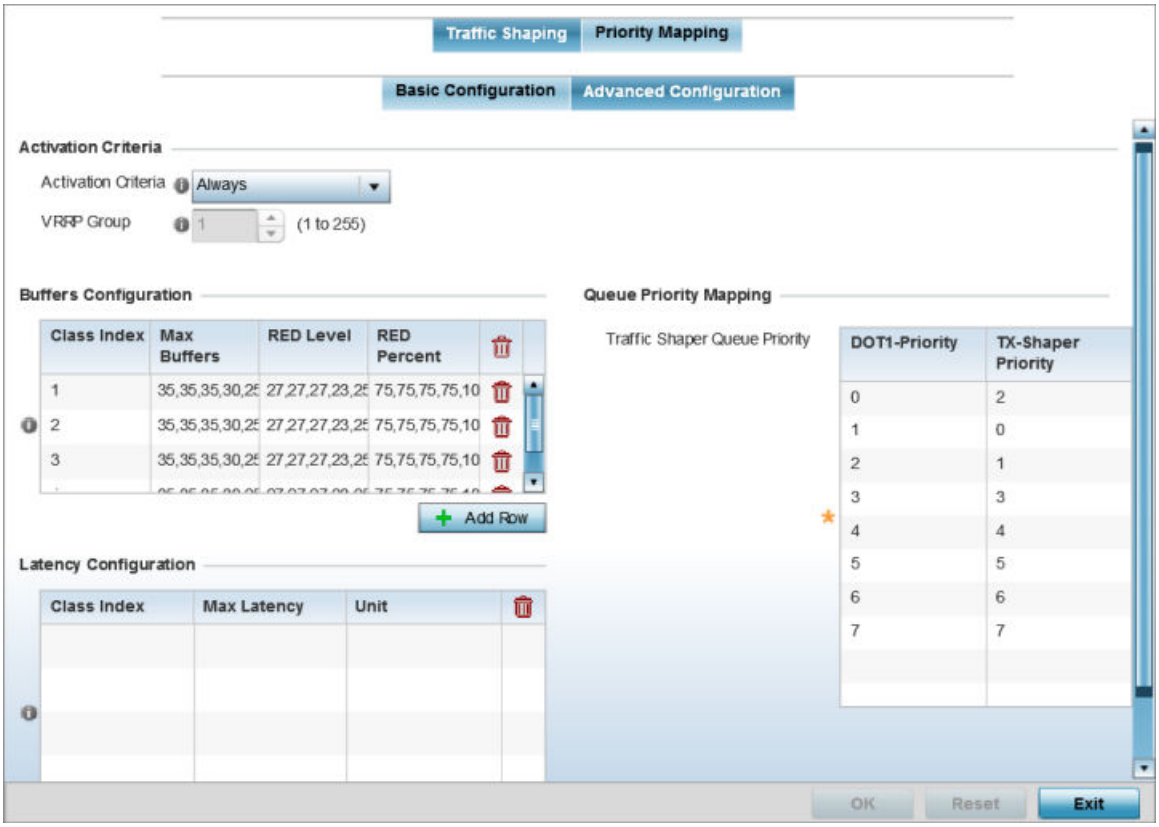



**Figure 184: QoS - Traffic Shaping - Advanced Configuration Screen**

2 In the Activation Criteria field, set the following traffic shaper activation criteria:

| | |
|---|---|
| Activation Criteria | Use the drop-down menu to determine when the traffic shaper is invoked. Options include: **vrrp-master**, **cluster-master**, **rf-domain-manager** and **Always**. A VRRP master responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. The solitary cluster master is the cluster member elected, using a priority assignment scheme, to provide management configuration and Smart RF data to other cluster members. Cluster requests go through the elected master before dissemination to other cluster members. The RF Domain manager is the elected member capable of storing and provisioning configuration and firmware images for other members of the RF Domain. |
| VRRP Group | Set the VRRP group ID from 1 - 255. VRRP groups is only enabled when the Establishment Criteria is set to vrrp-master. |

3 In the Buffers Configuration table, click **+ Add Row** and set the following:

| | |
|---|---|
| Class Index | Set a class index from 1 - 4. |
| Max Buffers | Set this value to specify the queue length limit after which the queue starts to drop packets. Set the maximum queue lengths for packets. The upper length is 400 for access points. |
| RED Level | Set the packet queue length for RED. The upper limit is 400 for access points. The rate limiter uses the RED *(random early detection )* algorithm for rate limiting traffic. RED is a queueing technique for congestion avoidance. RED monitors the average queue size and drops or marks packets. If the buffer is near empty, all incoming packets are accepted. When the queue grows, the probability for dropping an incoming packet also grows. When the buffer is full, the probability has reached 1 and all incoming packets are dropped. |
| RED Percent | Set a percentage (1 - 100) for RED rate limiting at a percentage of maximum buffers. |

4 Select **+ Add Row** within the Latency Configuration table to set the Class Index (1 - 4), Max Latency and latency measurement Unit. Max latency specifies the time limit after which packets start dropping (maximum packet delay in the queue). The maximum number of entries is 8. Select whether msec (default) or usec is unit for latency measurement.

When a new packet arrives it knows how much time to wait in the queue. If a packet takes longer than the latency value, it is dropped. By default latency is not set, so packets remain in queue for long time.

5 Refer to the Queue Priority Mapping table to set the traffic shaper queue priority and specify a particular queue inside a class. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets mark 802.1p markings.

6 Select **OK** to save the traffic shaping advanced configuration changes.

Select **Reset** to revert to the last saved configuration.

Profile Overrides - Priority Mapping

1 Select the **Priority Mapping** tab.

The **Quality of Service (QoS) → Priority Mapping** screen displays.

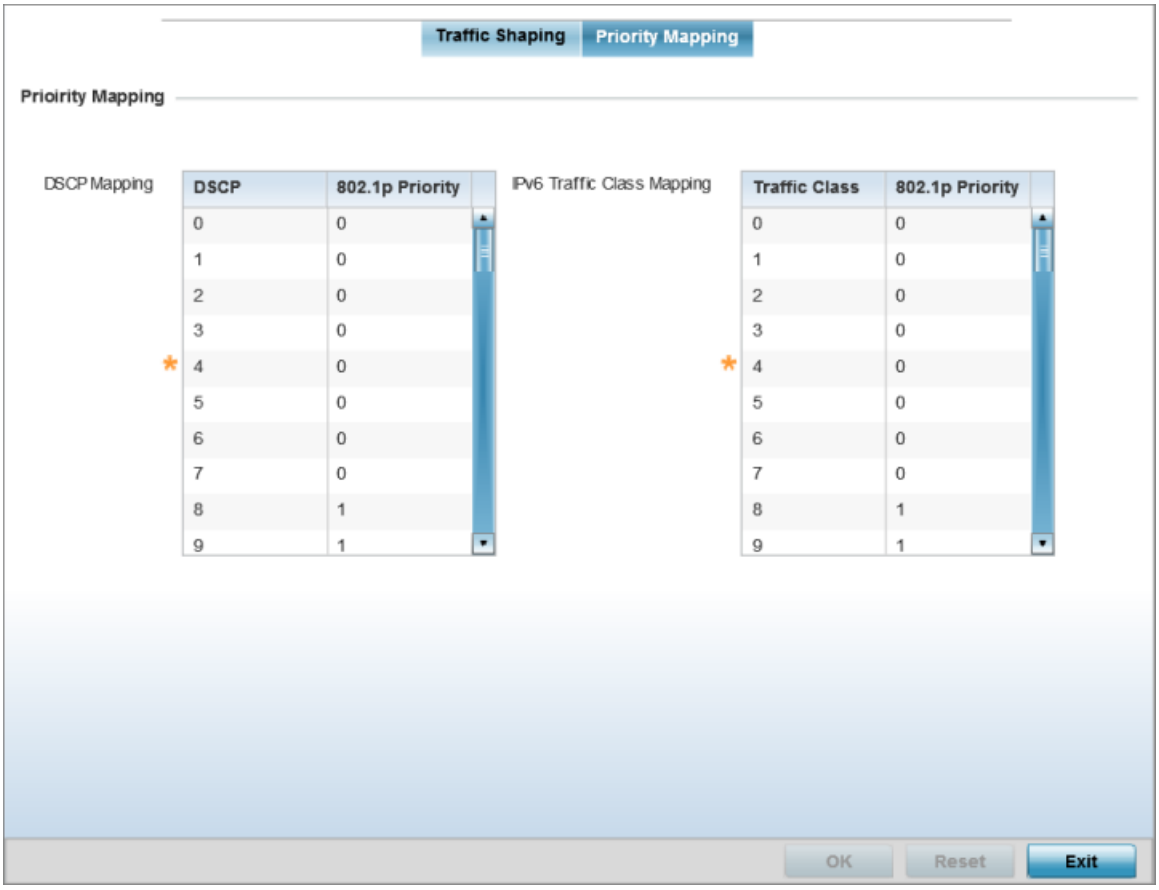



**Figure 185: QoS - Priority Mapping Configuration Screen**

2 In the DSCP Mapping table, set the following IP DSCP mappings for untagged frames:

| | |
|---|---|
| DSCP | Lists the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. |
| 802.1p Priority | Assign a 802.1p priority as a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are:<br>• 0 – *Best Effort*<br>• 1 – *Background*<br>• 2 – *Spare*<br>• 3 – *Excellent Effort*<br>• 4 – *Controlled Load*<br>• 5 – *Video*<br>• 6 – *Voice*<br>• 7 – *Network Control*<br><br>Note:<br>Use the spinner controls within the **802.1p Priority** field for each DSCP row to change its priority value. |

3 In the IPv6 Traffic Class Mapping table, set or override the following IPv6 DSCP settings for untagged frames:

| | |
|---|---|
| Traffic Class | Devices that originate a packet must identify different classes or priorities for IPv6 packets. Devices use the traffic class field in the IPv6 header to set this priority. |
| 802.1p Priority | Assign a 802.1p priority as a 3-bit IPv6 precedence value in the Type of Service field of the IPv6 header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are:<br>• 0 – *Best Effort*<br>• 1 – *Background*<br>• 2 – *Spare*<br>• 3 – *Excellent Effort*<br>• 4 – *Controlled Load*<br>• 5 – *Video*<br>• 6 – *Voice*<br>• 7 – *Network Control* |

4 Select **OK** to save the priority mapping changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - Spanning Tree

The STP *(Spanning Tree Protocol)*, standardized in IEEE 802.1D, is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include backup links to provide fault tolerance if an active link fails.

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **Spanning Tree**.

The Spanning Tree configuration screen displays.

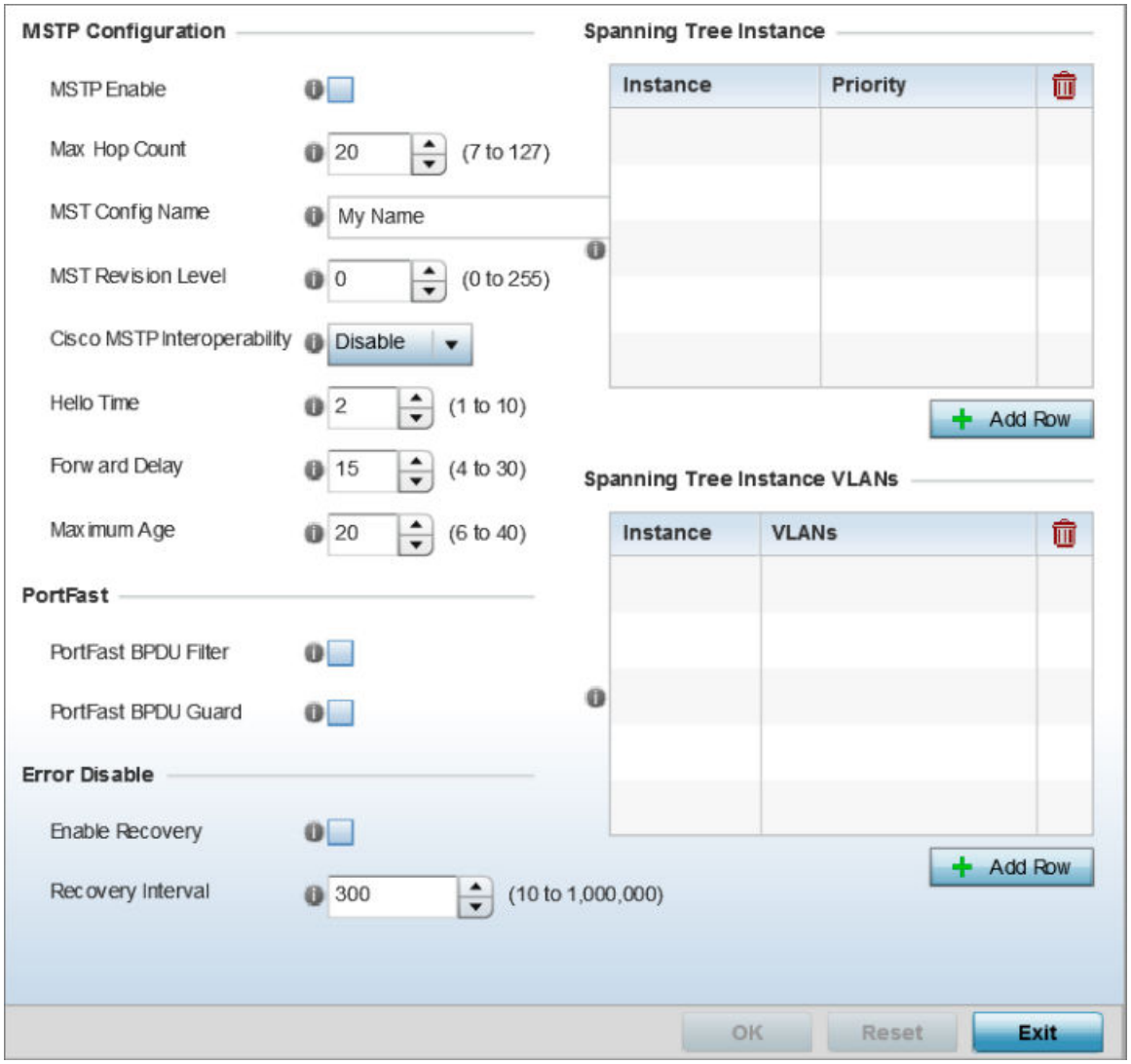



**Figure 186: Spanning Tree Configuration Screen**

4 Set the following MSTP Configuration parameters:

| | |
|---|---|
| MSTP Enable | Select this option to enable MSTP for this profile. MSTP is disabled by default, so if requiring different (groups) of VLANs with the profile supported network segment. |
| Max Hop Count | Define the maximum number of hops the BPDU will consider valid in the spanning tree topology. The available range is from 7 - 127. The default setting is 20. |
| MST Config Name | Define a 64 character maximum name for the MST region as an identifier. |
| MST Revision Level | Set a numeric revision value ID for MST configuration information. Set a value from 0 - 255. The default setting is 0. |

| | |
|---|---|
| Cisco MSTP Interoperability | Select either the **Enable** or **Disable** radio buttons to enable/disable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default. |
| Hello Time | Set a BPDU hello interval from 1 - 10 seconds. BPDUs are exchanged regularly (every 2 seconds by default) and enable supported devices to keep track of network changes and star/stop port forwarding as required. |
| Forward Delay | Set the forward delay time from 4 - 30 seconds. When a device is first attached to a port, it does not immediately start to forward data. It first processes BPDUs and determines the network topology. When a host is attached the port always goes into the forwarding state, after a delay of while it goes through the listening and learning states. The time spent in the listening and learning states is defined by the forward delay (15 seconds by default). |
| Maximum Age | Use the spinner control to set the maximum time (in seconds) to listen for the root bridge. The root bridge is the spanning tree bridge with the smallest (lowest) bridge ID. Each bridge has a unique ID and a configurable priority number, the bridge ID contains both. The available range is from 6 - 40. The default setting is 20. |

5 Define the following Port Fast parameters:

| | |
|---|---|
| PortFast BPDU Filter | Enable to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. BPDUs are exchanged regularly and enable the access point to keep track of network changes and to start and stop port forwarding as required. This option is disabled by default. |
| PortFast BPDU Guard | Enable to invoke a BPDU guard for the portfast enabled port. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. BPDUs are exchanged regularly and enable the access point to keep track of network changes and to start and stop port forwarding as required. This option is disabled by default. |

6 Define the following Error Disable settings:

| | |
|---|---|
| Enable Recovery | Select this option to enable a error disable timeout resulting from a BPDU guard. This setting is disabled by default. |
| Recovery Internal | Define the recovery interval used to enable disabled ports. The available range is from 10 - 1,000,000 seconds with a default setting of 300. |

7 Use the Spanning Tree Instance table to add indexes to the spanning tree topology.

Add up to 16 indexes and use the Priority setting to define the bridge priority used to determine the root bridge. The lower the setting defined, the greater the likelihood of becoming the root bridge in the spanning tree topology.

8 Use the Spanning Tree Instance VLANs table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.

9 Select the **OK** to save the STP changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - IPv4 Routing

Routing is the process of selecting IP paths to send access point managed network traffic. Use the Routing screen to set destination IP and gateway addresses enabling assignment of static IP addresses for requesting clients without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file and reduces the resource space required to maintain address pools.

Both IPv4 and IPv6 routes are separately configurable using their appropriate tabs. For IPv6 networks, routing is the part of IPv6 that provides forwarding between hosts located on separate segments within a larger IPv6 network where IPv6 routers provide packet forwarding for other IPv6 hosts.

To override the access point profile's static routes:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides → Network** and select **Routing**.

The IPv4 Routing configuration screen displays.

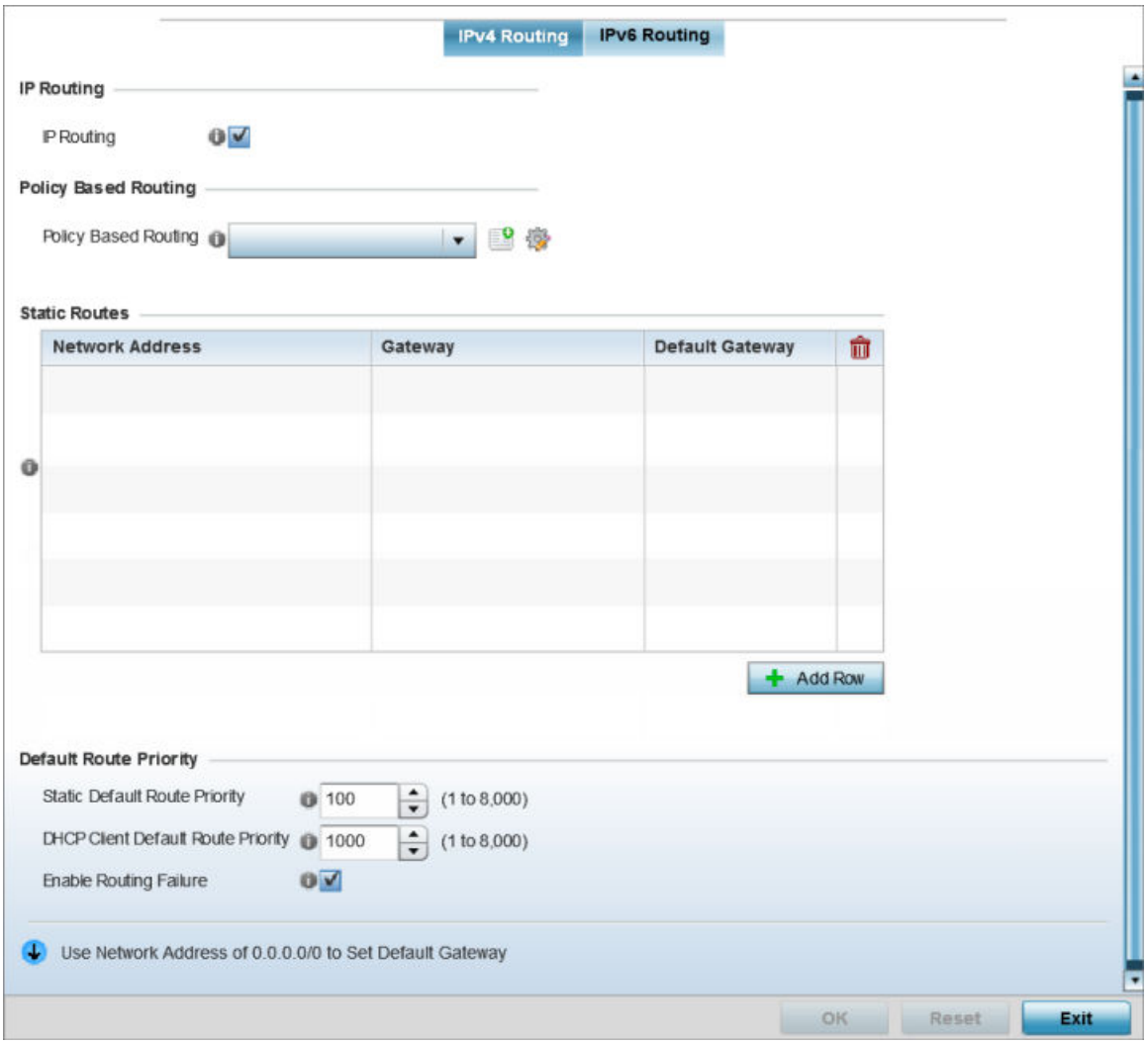



**Figure 187: Profile Overrides - IPv4 Routing Configuration Screen**

4 Select **IP Routing** to enable static routes using IPv4 addresses. This option is enabled by default.

5 In the Policy Based Routing field, use the Policy Based Routing drop-down menu to apply a policy. Select the **Create** icon to create a policy based route or select the **Edit** icon to edit an existing policy after selecting it in the drop-down list. For more information on creating a Policy Based Routing Policy, see Policy Based Routing (PBR) on page 676.

6 in the Statis Routes table, click **Add Row +** and provide the following statis route details:

| | |
|---|---|
| Network Address | Add network IP addresses and network masks |
| Gateway | Provide the Gateway's IP address. This is the gateway used to route traffic to the specified network. |
| Default Gateway | Provide the Default Gateway's IP address. This is the gateway used to route traffic to the specified network. |

7 In the Default Route Priority field, and set the following parameters:

| | |
|---|---|
| Static Default Route Priority | Use the spinner control to set the priority value (1 - 8,000) for the default static route. This is weight assigned to this route versus others that have been defined. The default setting is 100. |
| DHCP Client Default Route Priority | Use the spinner control to set the priority value (1 - 8,000) for the default route learnt from the DHCP client. The default setting is 1000. |
| Enable Routing Failure | When selected, all default gateways are monitored for activity. The system will failover to a live gateway if the current gateway becomes unusable. This feature is enabled by default. |

8 Select the **OK** button to save the IPv4 routing configuration changes.

Select **Reset** to revert to the last saved configuration.

Profile Overrides - IPv6 Routing

1 Select the **IPv6 Routing** tab.

IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.

The IPv6 Routing configuration screen displays.

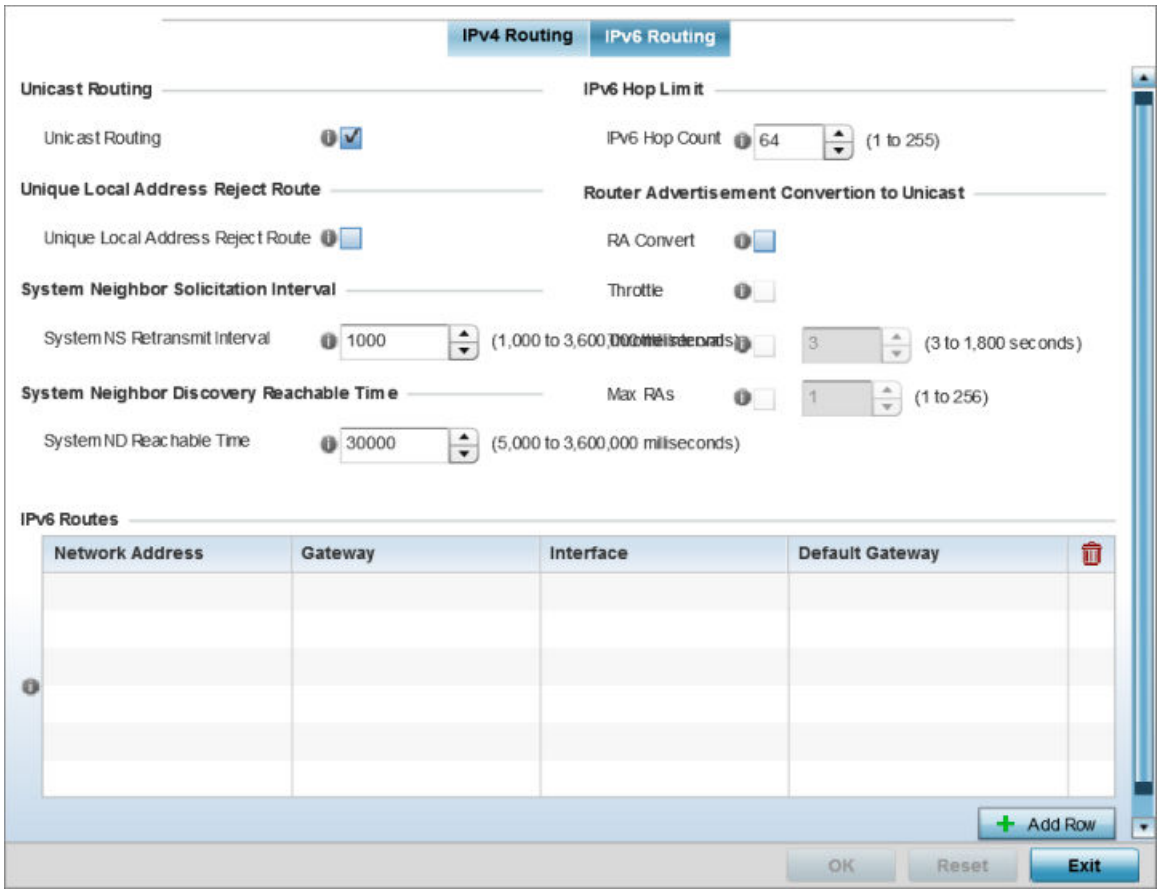



**Figure 188: IPv6 Routing COnfiguration Screen**

2 Select Unicast Routing to enable IPv6 unicast routing for this profile. Keeping unicast enabled allows the profile's neighbor advertisements and solicitations in unicast (as well as multicast) to provide better neighbor discovery. This setting is enabled by default.

3 Select Unique Local Address Reject Route to enable rejecting local routes in the format FC00::/7.

4 Set a System NS Retransmit Interval (from 1,000 to 3,600,000 milliseconds) as the interval between NS *(neighbor solicitation)* messages. NS messages are sent by a node to determine the link layer address of a neighbor, or verify a neighbor is still reachable via a cached link-layer address. The default is 1,000 milliseconds.

5 Set a System ND Reachable Time (from 5,000 to 3,600,000 milliseconds) as the time a neighbor is assumed to be reachable after receiving a receiving a ND *(neighbor discovery)* confirmation for their reachability. The default is 30,000 milliseconds.

6 Set an IPv6 Hop Count (from 1 - 255) as the maximum number of hops considered valid when sending IP packets. The default setting is 64.

7 Set the following **Router Advertisement Conversion to Unicast** settings:

| | |
|---|---|
| RA Convert (milliseconds) | Select this option to convert multicast router advertisements (RA) to unicast router advertisements at the dot11 layer. Unicast addresses identify a single network interface, whereas a multicast address is used by multiple hosts. This setting is disabled by default. |
| Throttle | Select this option to throttle RAs before converting to unicast. Once enabled, set the throttle interval and maximum number of RAs. This setting is disabled by default. |
| Throttle Interval (milliseconds) | Enable this setting to define the throttle interval (3 - 1,800 seconds). The default setting is 3 seconds. |
| Max RAs | Enable this setting to define the maximum number of router advertisements per router (1 - 256) during the throttle interval. The default setting is 1. |

8 In the **IPv6 Routes** table, click **+ Add Row** and add additional 256 IPv6 route resources.

The IPv6 static route **Add Row** screen displays.

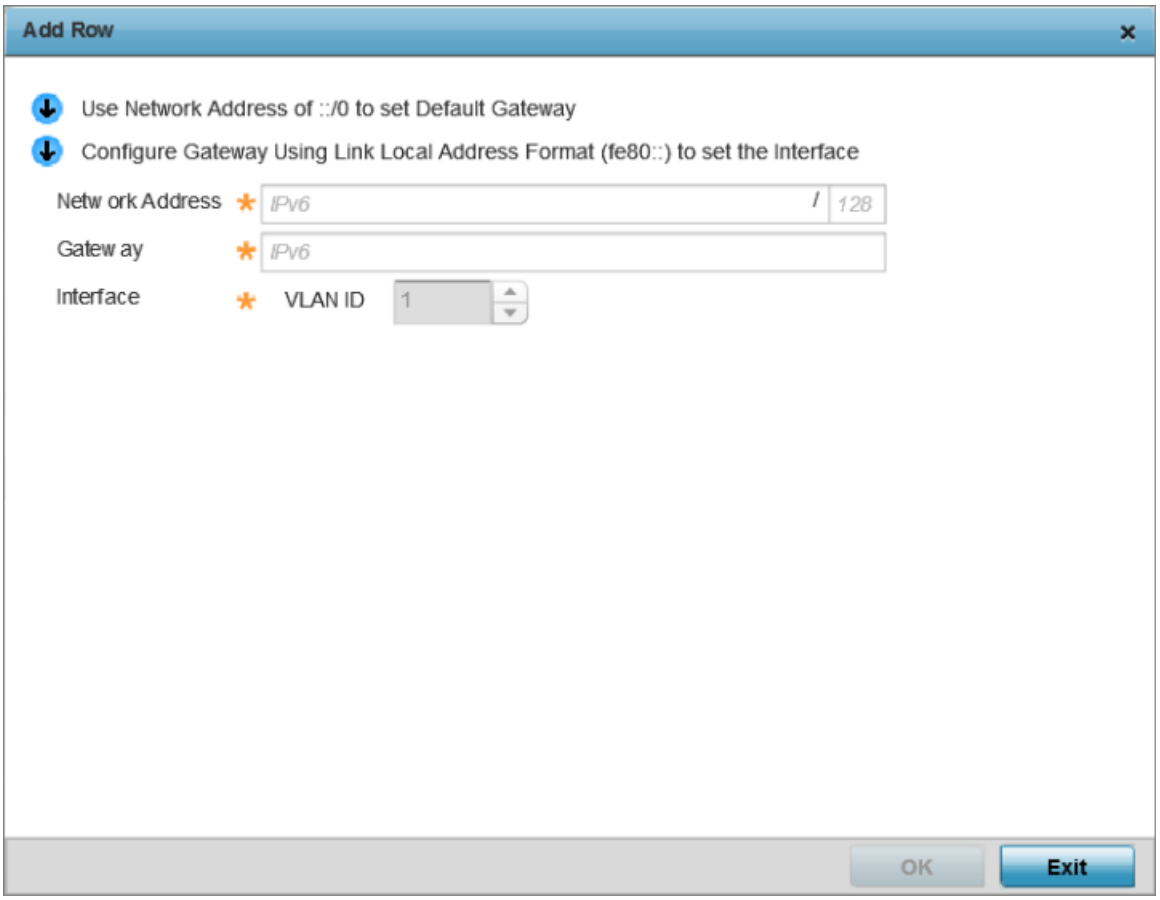



**Figure 189: Add IPv6 Static Route Window**

| | |
|---|---|
| Network Address | Set the IPv6 network address. Other than the length and slightly different look versus an IPv4 address, the IPv6 address concept is same as IPv4. |
| Gateway | Set the IPv6 route gateway. A network gateway in IPv6 is the same as in IPv4. A gateway address designates how traffic is routed out of the current subnet. |
| Interface | If using a link local address, set the VLAN (1 - 4,094) used a virtual routing interface for the local address. |

9 Select **OK** to save the IPv6 static route changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - OSPF Settings

OSPF *(Open Shortest Path First)* is a link-state IGP *(interior gateway protocol)*. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

To override an access point's profile OSPF configurations:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **OSPF**.

The **OSPF** → **OSPF Settings** configuration screen displays.

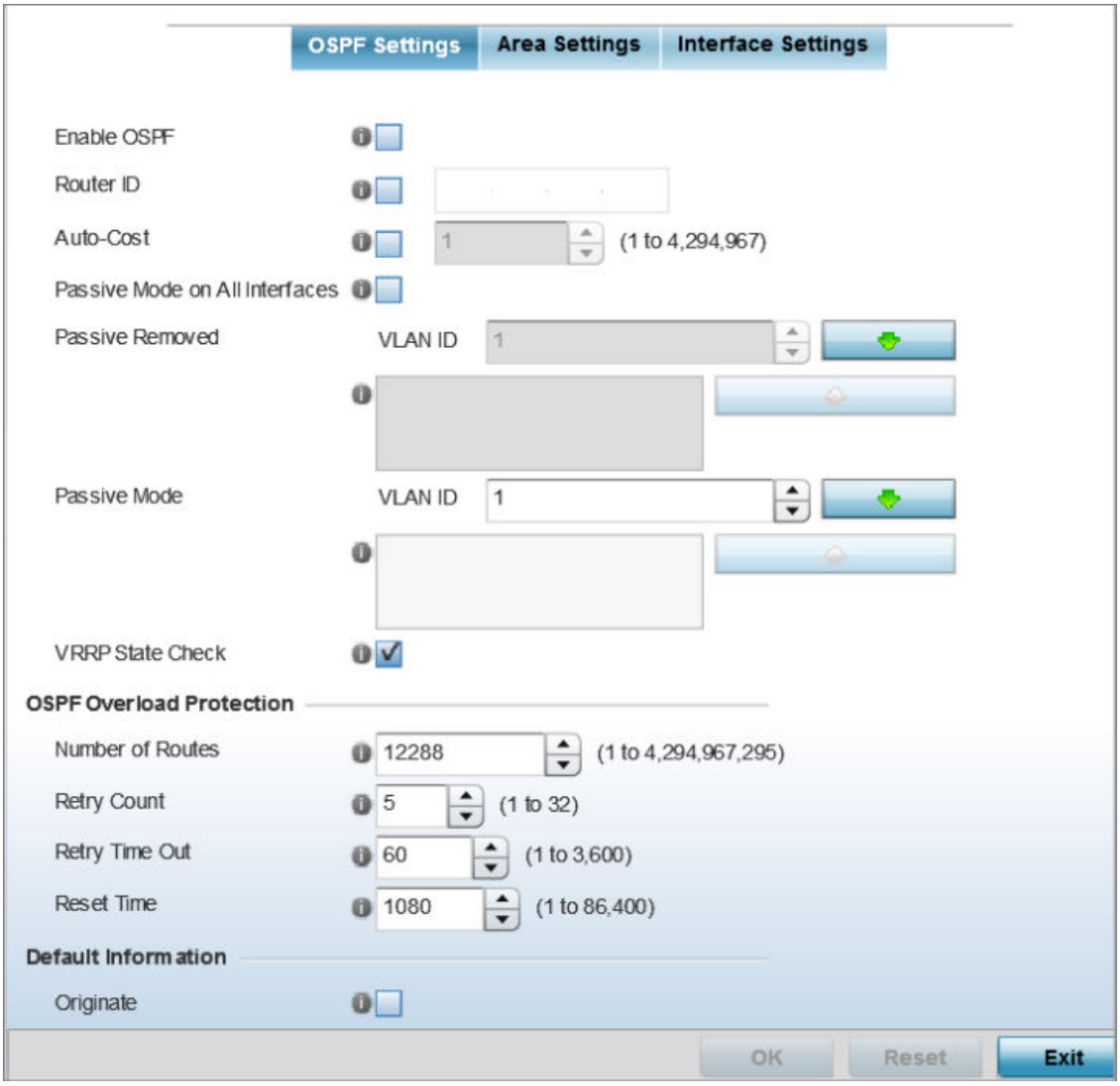



**Figure 190: Profile Overrides - OSPF Settings Configuration Screen**

4 Select the **Enable OSPF** check box, and provide the following dynamic routing settings:

| | |
|---|---|
| Router ID | Select this option to define a router ID (numeric IP address). This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network. |
| Auto-Cost | Select this option to specify the reference bandwidth (in Mbps) used to calculate the OSPF interface cost if OSPF is either STUB or NSSA. The default setting is 1. |
| Passive Mode on All Interfaces | When selected, all layer 3 interfaces are set as an OSPF passive interface. This setting is disabled by default. |

| | |
|---|---|
| Passive Removed | If *enabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF *non* passive interfaces. Multiple VLANs can be added to the list. |
| Passive Mode | If *disabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF passive interfaces. Multiple VLANs can be added to the list. |
| VRRP State Check | Select this option to enable checking of VRRP state. If the interface's VRRP state is not **`Backup`**, then the interface is published via OSPF. |

5 Set the following OSPF Overload Protection parameters:

| | |
|---|---|
| Number of Routes | Use the spinner controller to set the maximum number of OSPN routes permitted. The available range is from 1 - 4,294,967,295. |
| Retry Count | Set the maximum number of retries (OSPF resets) permitted before the OSPF process is shut down. The available range is from 1 - 32. The default setting is 5. |
| Retry Time Out | Set the duration (in seconds) the OSPF process remains off before initiating its next retry. The available range is from 1 - 3,600 seconds. The default is 60 seconds. |
| Reset Time | Set the reset time (in seconds) that, when exceeded, changes the retry count is zero. The available range is from 1 - 86,400. The default is 360 seconds. |

6 Set the following Default Information:

| | |
|---|---|
| Originate | Select this option to make the default route a distributed route. This setting is disabled by default. |
| Always | Enabling this setting continuously maintains a default route, even when no routes appear in the routing table. This setting is disabled by default. |
| Metric Type | Select this option to define the exterior metric type (**1** or **2**) used with the default route. |
| Route Metric | Select this option to define route metric used with the default route. OSPF uses path cost as its routing metric. It's defined by the speed (bandwidth) of the interface supporting a given route. |

7 In the Route Redistribution table, click **+ Add Row** and set the types of routes that can be used by OSPF.

| | |
|---|---|
| Route Type | Set the *Route Type* used to define the redistributed route. Options include: **`connected`**, **`kernel`** and **`static`**. |
| Metric Type | Select this check box, and define the exterior metric type (1 or 2) used with the route redistribution. |
| Metric | Select this option, and define route metric used with the redistributed route. |

8 In the OSPF Network table, click **+Add Row** and configure the following:

| | |
|---|---|
| Network | Add the IP address and mask of the Network(s) participating in OSPF. |
| Area ID | Define the OSPF area (IP address) to which the network belongs. |

9 In the Clear OSPF Process, click **Clear** to clear all OSPF Routing table entries.

10 Set an **OSPF Default Route Priority** (1 - 8,000) as the priority of the default route learnt from OSPF. The default priority is 7000.

11 Click **OK** to save the OSPF setting changes.

Click **Reset** to revert to the last saved configuration.

OSPF - Area Settings

An OSPF Area contains a set of routers exchanging LSAs *(Link State Advertisements)* with others in the same area. Areas limit LSAs and encourage aggregate routes.

To override the access point profile's OSPF area settings:

1 Select the **Area Settings** tab.

The OSPF Area main screen displays. This screen lists existing OSPF Area configurations.

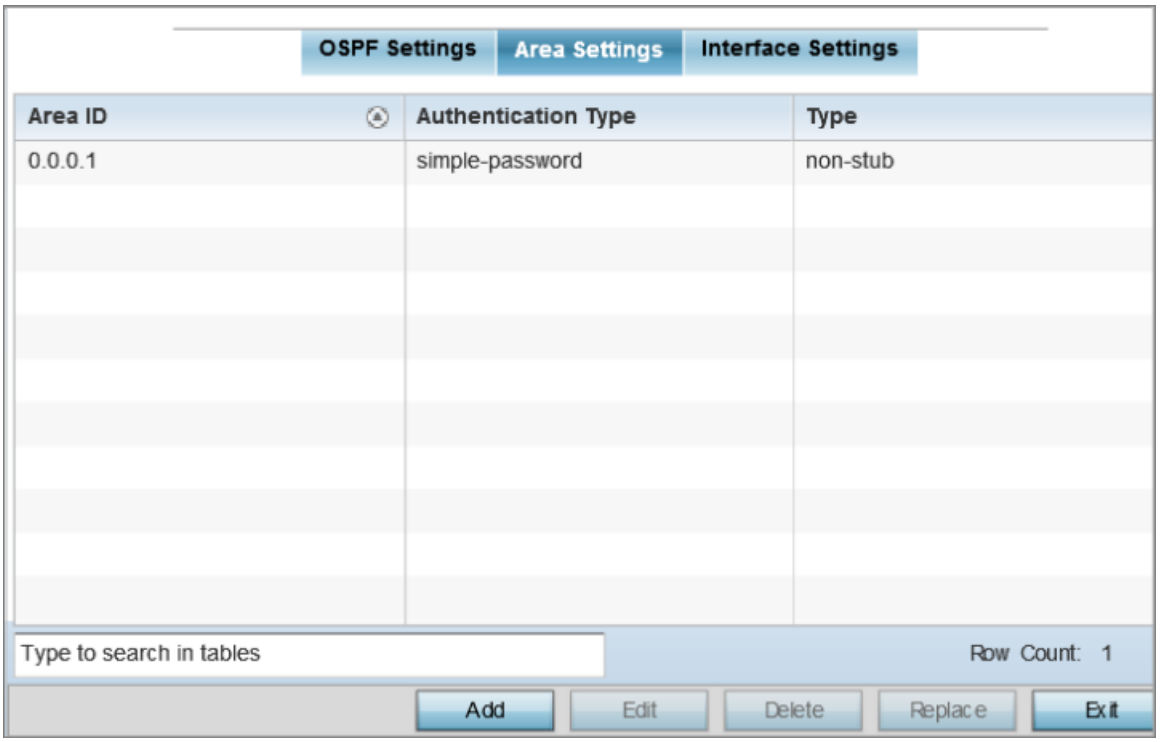



**Figure 191: OSPF - Area Setting Configuration Screen**

2 Review existing Area Settings configurations:

| | |
|---|---|
| Area ID | Displays either the IP address or integer representing the OSPF area. |
| Authentication Type | Lists the authentication schemes used to validate the credentials of dynamic route connections. |
| Type | Lists the OSPF area type in each listed configuration. |

3 To apply overrides, select an area entry from those listed on the screen, and click **Edit**.

You can also add new area configurations or delete existing configurations.

The add/edit OSPF Area screen displays.

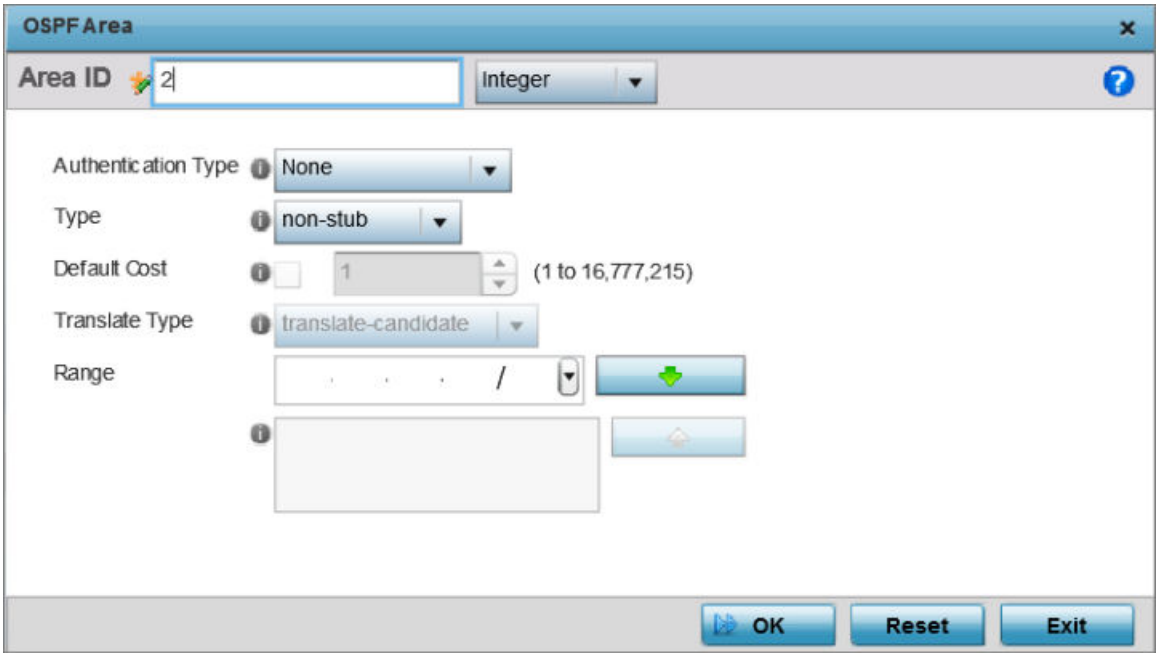



**Figure 192: OSPF - Add/Edit OSPF Area Configuration Screen**

4 Set the OSPF Area configuration.

| | |
|---|---|
| Area ID | Use the drop-down menu and specify either an IP address or Integer for the OSPF area. |
| Authentication Type | Select either **None**, **simple-password** or **message-digest** as credential validation scheme used with the OSPF dynamic route. The default setting is *None*. |
| Type | Set the OSPF area type as either **stub**, **totally-stub**, **nssa**, **totally-nssa** or **non-stub**. |
| Default Cost | Select this option to set the default summary cost advertised if creating a stub. Set a value from 1 - 16, 777,215. |
| Translate Type | Define how messages are translated. Options include **translate-candidate**, **translate-always** and **translate-never**. The default setting is *translate-candidate*. |
| Range | Specify a range of addresses for routes matching address/mask for OSPF summarization. |

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

Click **Reset** to revert to the last saved configuration.

OSPF - Interface Settings

To override the access point profile's OSPF interface settings:

1 Select the **Interface Settings** tab.

The OSPF interface configuration displays.

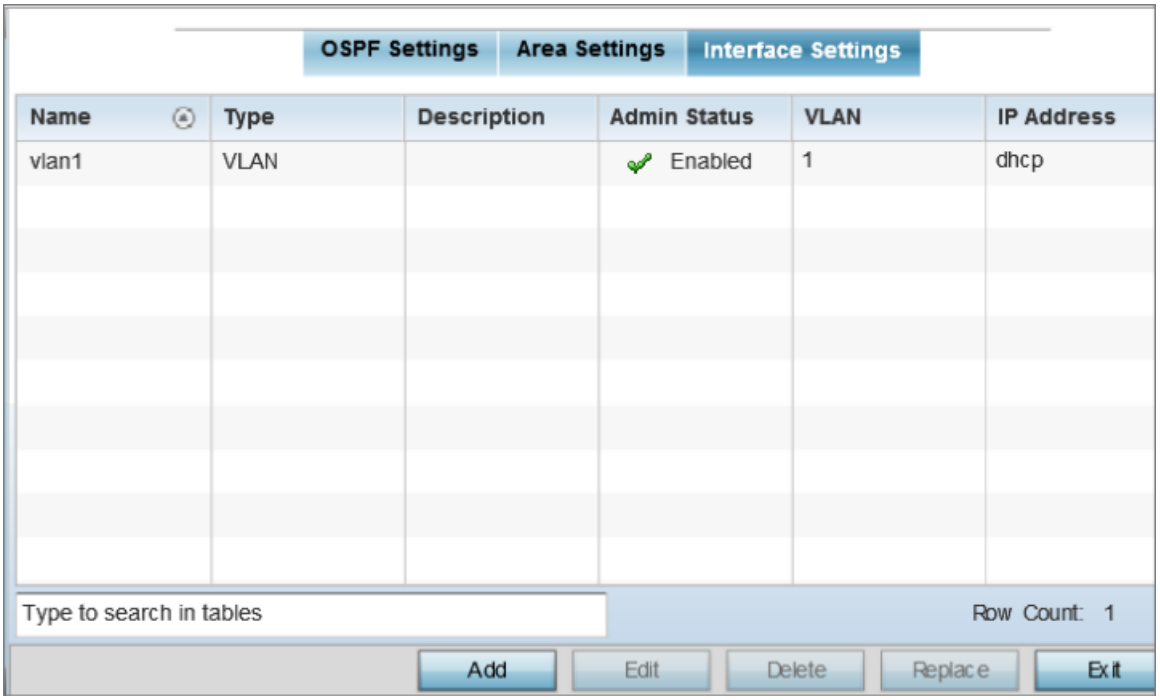



**Figure 193: OSPF - Interface Main Screen**

2 Review existing Interface Settings.

| | |
|---|---|
| Name | Displays the name defined for the interface configuration. |
| Type | Displays the type of interface. |
| Description | Lists each interface's 32 character maximum description. |
| Admin Status | A green check mark defines the interface as active and currently enabled with the profile. A red "X" defines the interface as currently disabled and not available for use. |
| VLAN | Lists the VLAN IDs set for each listed OSPF route virtual interface. |
| IP Address | Displays the IP addresses defined as virtual interfaces for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided. |

OSPF Basic General Settings

To add a new VLAN configuration or override an existing VLAN configuration:

1 Select **Add** or select the VLAN from those listed on the screen and click **Edit**.

You can also delete existing configurations.

The Basic Configuration screen displays, with the General tab selected by default.

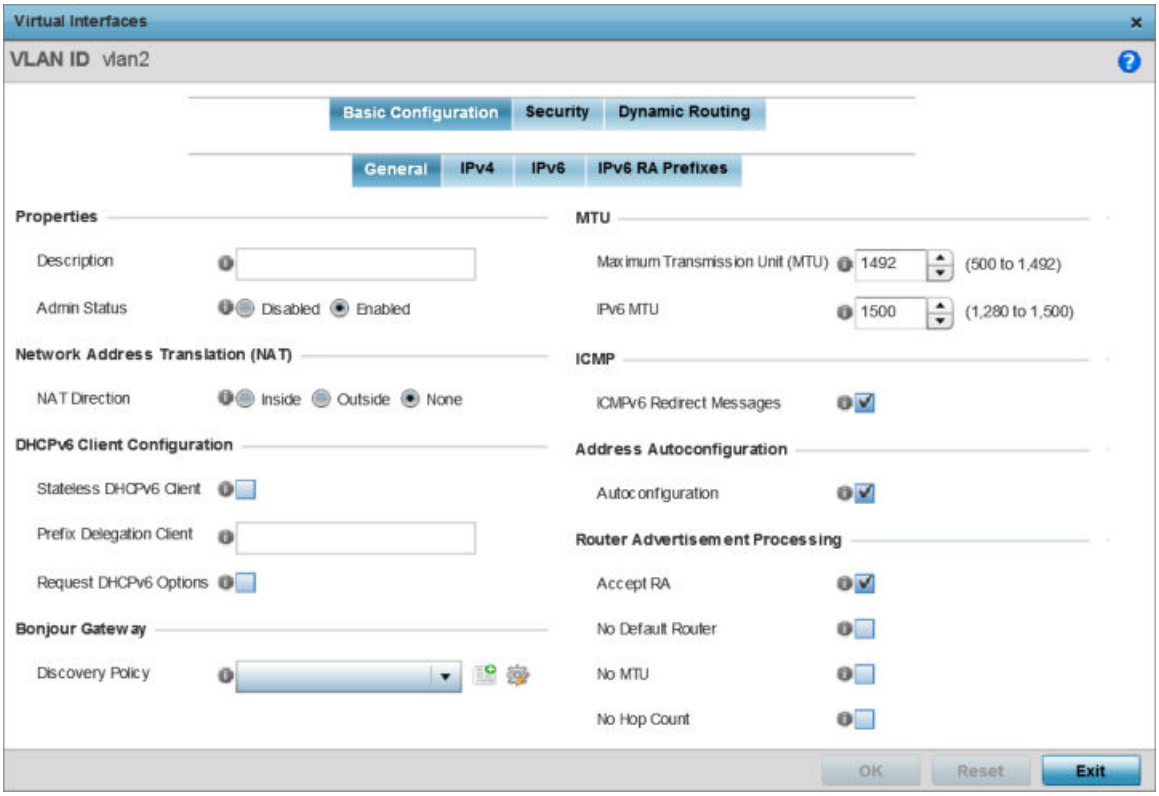



**Figure 194: OSPF - VLAN Interface Configuration Screen**

2 If creating a new Virtual Interface, use the **VLAN ID** spinner control to define a numeric ID from 1 - 4094.

3 Define the following parameters from within the Properties field:

| | |
|---|---|
| Description | Provide or edit a description (up to 64 characters) for the Virtual Interface that helps differentiate it from others with similar configurations. |
| Admin Status | Either select the **`Disabled`** or **`Enabled`** radio button to define this interface's current status within the network. When set to Enabled, the Virtual Interface is operational and available. The default value is Disabled. |

4 Define the Network Address Translation (NAT) direction.

Select one the following options:

- **`Inside`** - The inside network is transmitting data over the network to its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.
- **`Outside`** - Packets passing through the NAT on the way back to the LAN are searched against the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.
- **`None`** - No NAT activity takes place. This is the default setting.

5 Set the following **DHCPv6 Client Configuration** parameters:

The *Dynamic Host Configuration Protocol for IPv6* (DHCPv6) provides a framework for passing configuration information.

| | |
|---|---|
| Stateless DHCPv6 Client | Select this option to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default. |
| Prefix Delegation Client | Specify a 32 character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface. Devices use prefixes to distinguish destinations that reside on-link from those reachable using a router. |
| Request DHCPv6 Options | Select this option to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than locally. This setting is disabled by default. |

6 Set the following **MTU** settings:

| | |
|---|---|
| Maximum Transmission Unit (MTU) | Set the PPPoE client MTU from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492. |
| IPv6 MTU | Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500. |

7 Within the **ICMP** field, define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route. This setting is enabled by default.

8 Within the **Address Autoconfiguration** field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits. This setting is enabled by default.

9 Set the following **Router Advertisement Processing**settings for the virtual interface. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

| | |
|---|---|
| Accept RA | Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters. This setting is enabled by default. |
| No Default Router | Select this option to consider routers unavailable on this interface for default router selection. This setting is disabled by default. |

| | |
|---|---|
| No MTU | Select this option to *not use* the existing MTU setting for router advertisements on this virtual interface. If the value is set to zero no MTU options are sent. This setting is disabled by default. |
| No Hop Count | Select this option to *not use* the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default. |

10 Use the **Discovery Policy** drop-down menu to define the Bonjour Gateway Discovery Policy. Bonjour is Apple's service discovery protocol.

11 Select **OK** to save the changes to the basic configuration.

Select **Reset** to revert to the last saved configuration.

OSPF IPv4 Settings

IPv4 is a connectionless protocol. It operates on a best effort delivery model that does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

To set the VLAN IPv4 settings:

1 Select the **IPv4** tab.

The OSPF VLAN interface IPv4 configuration screen displays.

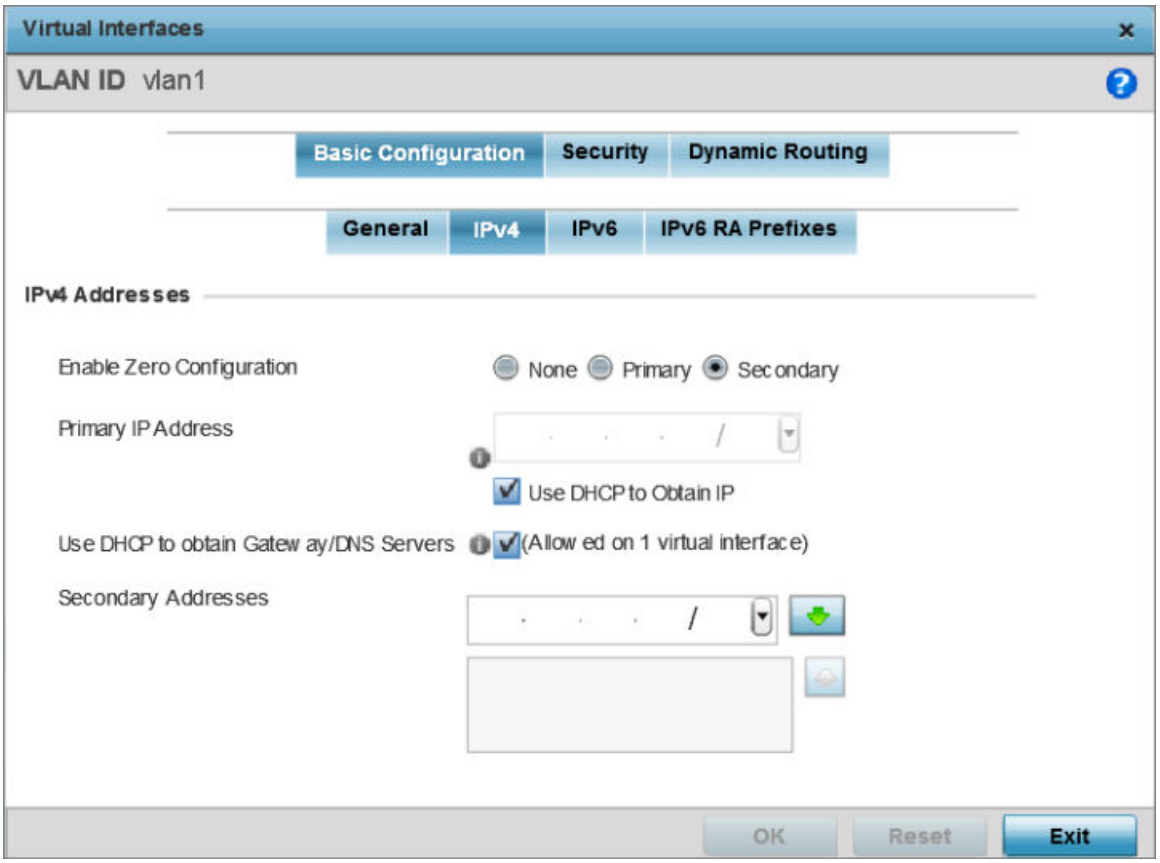



**Figure 195: OSPF - VLAN interface IPv4 Configuration Screen**

2 Set the following network information from within the IPv4 Addresses field:

| | |
|---|---|
| Enable Zero Configuration | Zero configuration can provide a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to None by default. |
| Primary IP Address | Define the IP address for the VLAN associated Virtual Interface. |
| Use DHCP to Obtain IP | Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field. |
| Use DHCP to obtain Gateway/DNS Servers | Select this option to allow DHCP to obtain a default gateway address and DNS resource for one virtual interface. This setting is disabled by default and only available when the Use DHCP to Obtain IP option is selected. |
| Secondary Addresses | Use this parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable. |

3 Select **OK** to save the changes to the IPv4 configuration.

Select **Reset** to revert to the last saved configuration.

OSPF IPv6 Settings

IPv6 is the latest revision of the *Internet Protocol* designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

To set the VLAN IPv6 settings:

1 Select the IPv6 tab to set IPv6 settings for this virtual interface.

The OSPF VLAN interface IPv6 configuration screen displays.

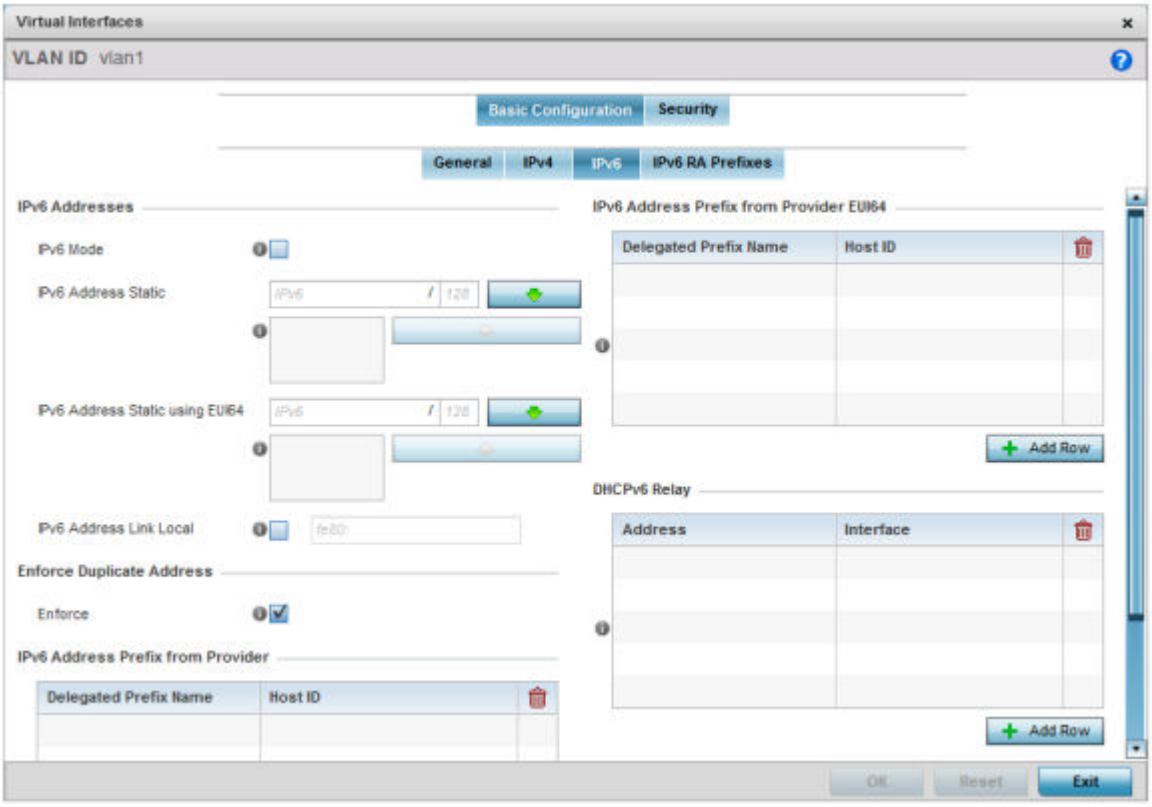



**Figure 196: OSPF - VLAN Interface IPv6 Configuration Screen**

2 Refer to the IPv6 Addresses field to define how IP6 addresses are created and utilized.

| | |
|---|---|
| IPv6 Mode | Select this option to enable IPv6 support on this virtual interface. IPv6 is disabled by default. |
| IPv6 Address Static | Define up to 15 global IPv6 IP addresses that can created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons. |
| IPv6 Address Static using EU164 | Optionally set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24-bits, with one being an OUI (Organizationally Unique Identifier) and the other being client specific. A 16- bit 0xFFFE is then inserted between the two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address. |
| IPv6 Address Link Local | Provide the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled, even when one or more routable addresses are assigned. |

3 Enable the Enforce Duplicate Address option to enforce duplicate address protection when any wired port is connected and in a forwarding state. This option is enabled by default.

4 In the IPv6 Address Prefix from Provider table, click **+ Add Row** and create IPv6 format prefix shortcuts as supplied by an ISP.

The IPv6 Address from Provider - Add Row screen displays.

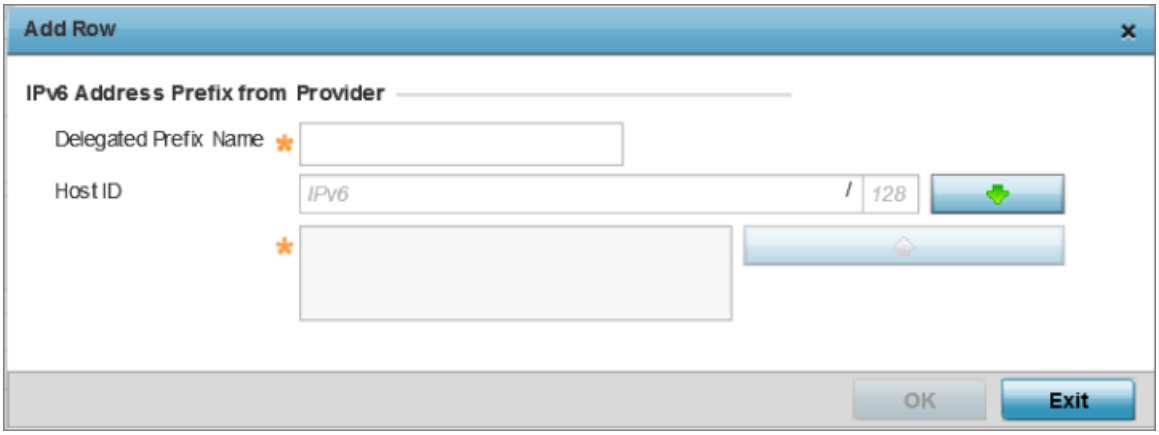



**Figure 197: OSPF - IPv6 Add IPv6 Address Prefix from Provider Screen**

| | |
|---|---|
| Delegated Prefix Name | Enter a 32 character maximum name for the IPv6 address prefix from provider. |
| Host ID | Define the subnet ID, host ID and prefix length. |

5 Select **OK** to save the IPv6 prefix from provider configuration changes.

Select **Exit** to close the screen without saving the updates.

6 In the IPv6 Address Prefix from Provider EUI64 table, click **+ Add Row** and set an (abbreviated) IP address prefix in EUI64 format.

The IPv6 Address from Provider EU164 - Add Row screen displays.

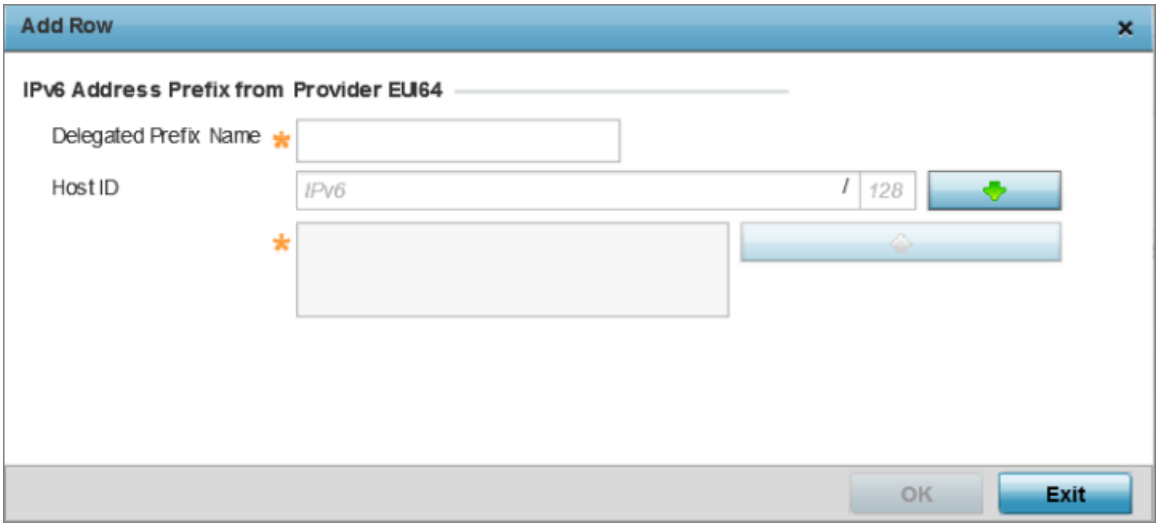



**Figure 198: OSPF - IPv6 Add Address Prefixes from Provider EU164**

| | |
|---|---|
| Delegated Prefix Name | Enter a 32 character maximum name for the IPv6 prefix from provider in EUI format. Using EUI64, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without manual configuration or DHCP. |
| Host ID | Define the subnet ID and prefix length. |

7 Select **OK** to save the IPv6 prefix from provider in EUI64 format changes.

Select **Exit** to close the screen without saving the updates.

8 Refer to the **DHCPv6 Relay** table to set the address and interface of the DHCPv6 relay.

The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

9 Select **+ Add Row** to launch a sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.

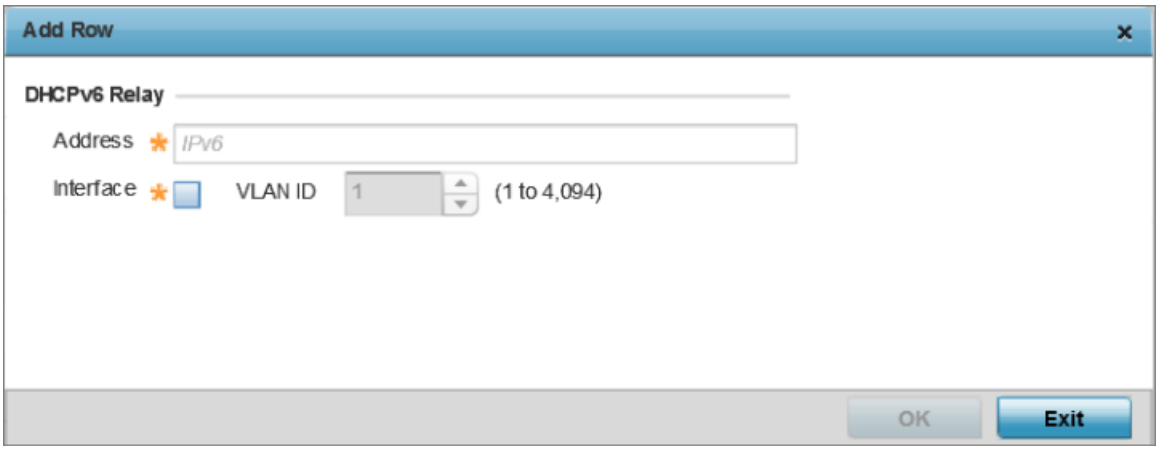



**Figure 199: OPSF - VLAN Interface DHCPv6 Relay Configuration Screen**

| | |
|---|---|
| Address | Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network. |
| Interface | Select this option to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available. |

10 Click **OK** to save the DHCPv6 relay configuration changes.

Click **Exit** to close the screen without saving the updates.

OSPF IPv6 RA Prefixes

To set the VLAN IPv6 RA Prefixes:

1 Select the **IPv6 RA Prefixes** tab.

The IPv6 RA Prefix configuration screen displays.

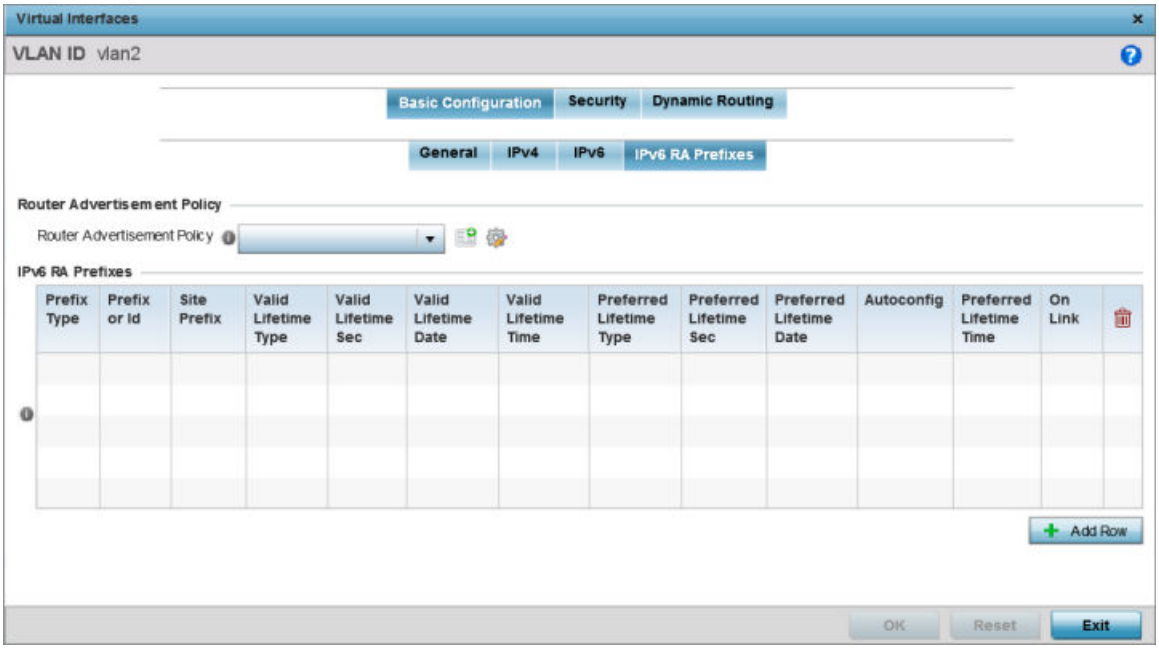



**Figure 200: OSPF - VLAN Interface IPv6 RA Prefix Configuration Screen**

2 Use the Router Advertisement Policy drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. For more information on Router Advertisement Policy, see IPv6 Router Advertisment Policy on page 704.

3 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

The add/edit IPv6 RA Prefixes configuration screen displays.

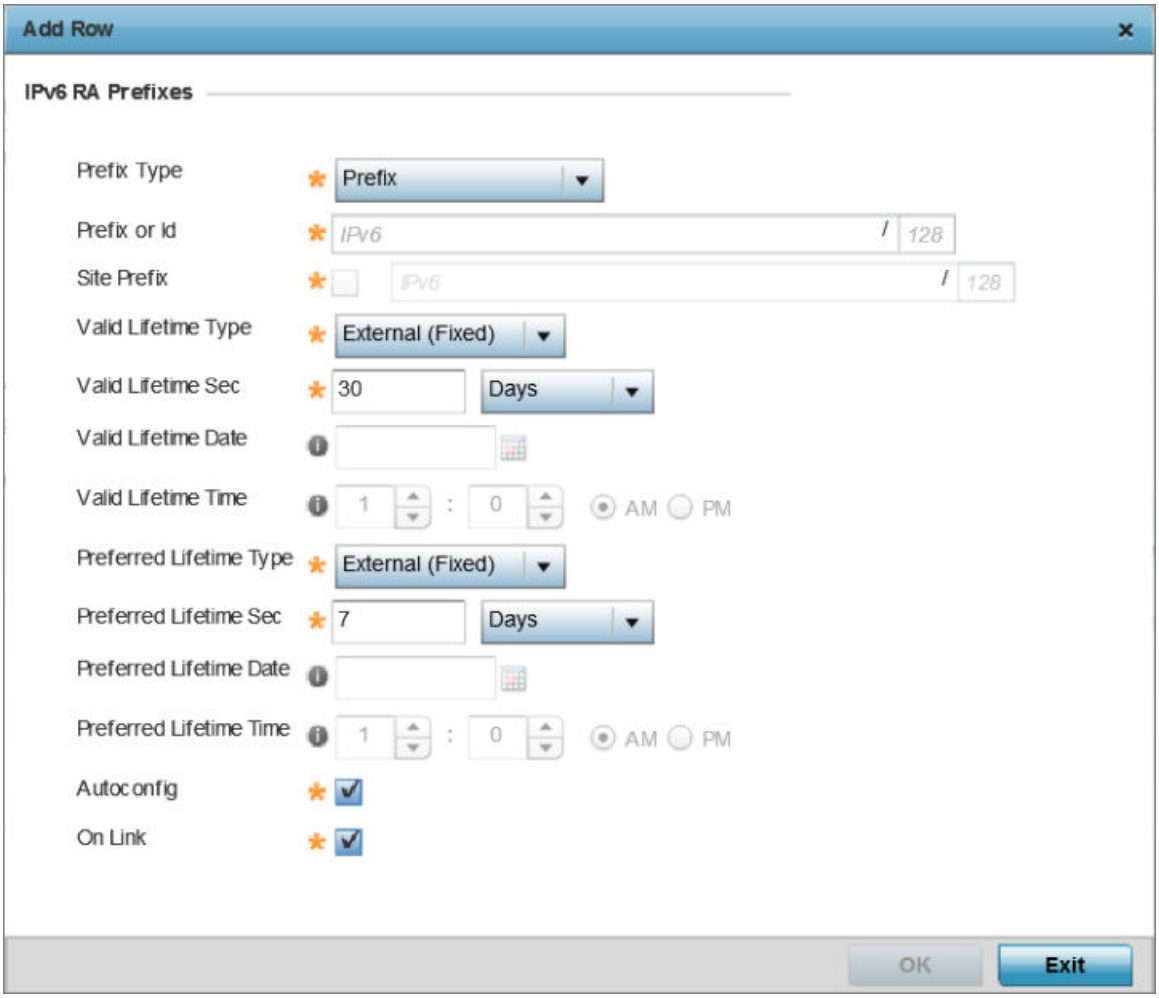



**Figure 201: Add/Edit IPv6 RA Prefixes Configuration Screen**

4 Set the following IPv6 RA Prefixes settings:

| | |
|---|---|
| Prefix Type | Set the prefix delegation type used with this configuration. Options include, Prefix, and prefix-from-provider. The default setting is Prefix. A prefix allows an administrator to associate a user defined name to an IPv6 prefix. A provider assigned prefix is made available from an ISP *(Internet Service Provider)* to automate the process of providing and informing the prefixes used. |
| Prefix or ID | Set the actual prefix or ID used with the IPv6 router advertisement. |
| Site Prefix | The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link. |

| | |
|---|---|
| Valid Lifetime Type | Set the lifetime for the prefix's validity. Options include **External (fixed)**, **decrementing** and **infinite**. If set to *External (fixed)*, just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to *decrementing*, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for *infinite*, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed). |
| Valid Lifetime Sec | If the lifetime type is set to *External (fixed)*, set the **Seconds**, **Minutes**, **Hours** or **Days** value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime. |
| Valid Lifetime Date | If the lifetime type is set to decrementing, set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Valid Lifetime Time | If the lifetime type is set to decrementing, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the AM PM radio buttons to set the appropriate hour. |
| Preferred Lifetime Type | Set the administrator preferred lifetime for the prefix's validity. Options include **External (fixed)**, **decrementing** and **infinite**. If set to *External (fixed)*, just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to *decrementing*, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for *infinite*, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is *External (fixed).* |
| Preferred Lifetime Sec | If the administrator preferred lifetime type is set to External (fixed), set the **Seconds**, **Minutes**, **Hours** or **Days** value used to measure criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime. |
| Preferred Lifetime Date | If the administrator preferred lifetime type is set to decrementing, set the date in MM/DD/YYYY format for the expiration of the prefix. |
| Preferred Lifetime Time | If the preferred lifetime type is set to decrementing, set the time for the prefix's validity. Use the spinner controls to set the time in hours and minutes. Use the AM PM radio buttons to set the appropriate hour. |
| Autoconfig | Autoconfiguration includes generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default. |
| On Link | Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled. |

5 Click **OK** to save the IPv6 RA prefix configuration changes.

Click **Exit** to close the screen without saving the updates.

OSPF VLAN Security Settings

To set the VLAN security settings:

1 Select the **Security** tab.

The VLAN Interface security configuration screen displays.

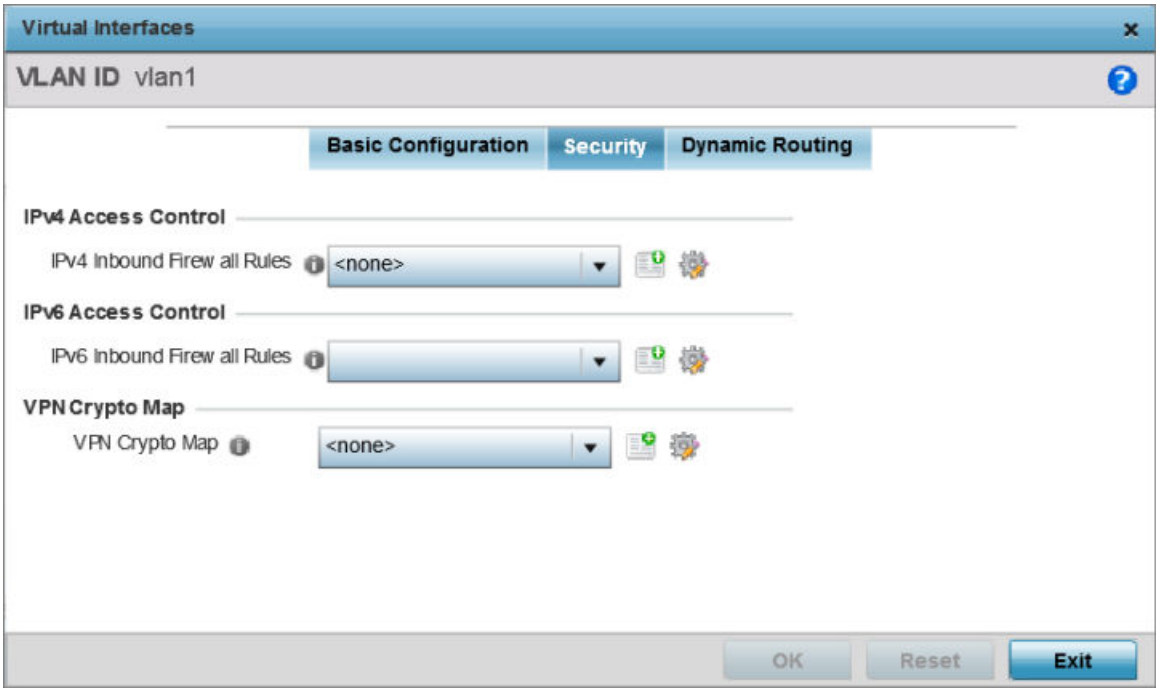



**Figure 202: OSPF - VLAN Interface Security Configuration Screen**

2 Use the **IPv4 Inbound Firewall Rules** drop-down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv4 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, since it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike TCP).

IPv4 and IPv6 are different enough to warrant separate protocols. IPv6 devices can alternatively use stateless address autoconfiguration. IPv4 hosts can use link local addressing to provide local connectivity. For more information on IPv4 firewall rules, see Configuring IP Firewall Rules on page 744.

3 Use the **IPv6 Inbound Firewall Rules** drop-down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv6 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv6 is the latest revision of the *Internet Protocol* replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. For more information on IPv6 firewall rules, see Configuring IP Firewall Rules on page 744.

4 Use the **VPN Crypto Map** drop-down menu to select and apply a VPN crypto map entry to apply to the OSPF dynamic route.

Crypto Map entries are sets of configuration parameters for encrypting packets passing through the VPN Tunnel. If a Crypto Map configuration does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new Crypto Map configuration or the **Edit** icon to modify an existing configuration.

5 Select **OK** to save the OSPF route security configuration changes.
Select **Reset** to revert to the last saved configuration.

OSPF Dynamic Routing Settings

To set the VLAN dynamic routing:

1 Select the **Dynamic Routing** tab.
The OSPF VLAN Interface Dynamic Routing configuration screen displays.

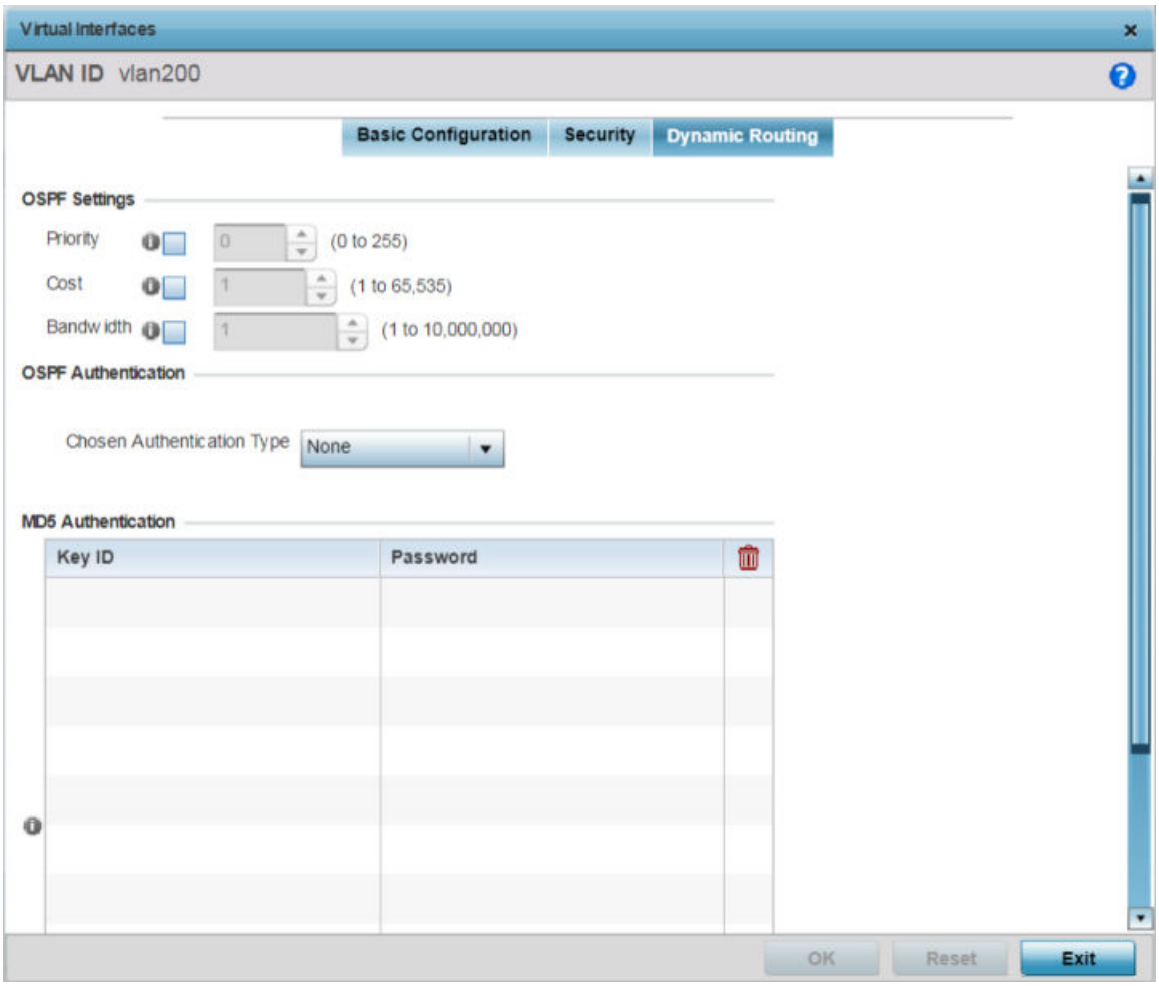



**Figure 203: OSPF - VLAN Interface Dynamic Routing Screen**

2 In the OSPF Settings field, override the following parameters:

| | |
|---|---|
| Priority | Select this option to set the OSPF priority used to select the network designated route. Use the spinner control to set the value from 0 - 255. |
| Cost | Select this option to set the cost of the OSPF interface. Use the spinner control to set the value from 1 - 65,535. |
| Bandwidth | Set the OSPF interface bandwidth (in Kbps) from 1 - 10,000,000. |

3 Use the Chosen Authentication Type drop-down to select the authentication type used to validate credentials within the OSPF dynamic route. Options include: **`simple-password`**, **`message-digest`**, **`null`** and **`None`**. The default is *None*.

4 In the MD5 Authentication table, click **+ Add Row** and configure the following:

MD5 is a message digest algorithm using a cryptographic hash producing a 128-bit (16-byte) hash value, usually expressed in text as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

| | |
|---|---|
| Key ID | Use the spinner control to set the OSPF message digest authentication key ID. The available range is from 1 - 255. |
| Password | Set the password (associated with the Key ID) used for an MD5 validation of authenticator credentials. The password is the OSPF key either displayed as series or asterisks. |

5 Click **OK** to save the IPv6 RA prefix configuration changes.

Click **Exit** to close the screen without saving the updates.

### Profile Overrides - Forwarding Database

A Forwarding Database forwards or filters packets on behalf of the managing controller, service platform or access point. The bridge reads the packet's destination MAC address and decides to either forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network segment, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to decide to filter or forward the packet.

To override an access point profile's forwarding database configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **Forwarding Database**.

The Forwarding Database configuration screen displays

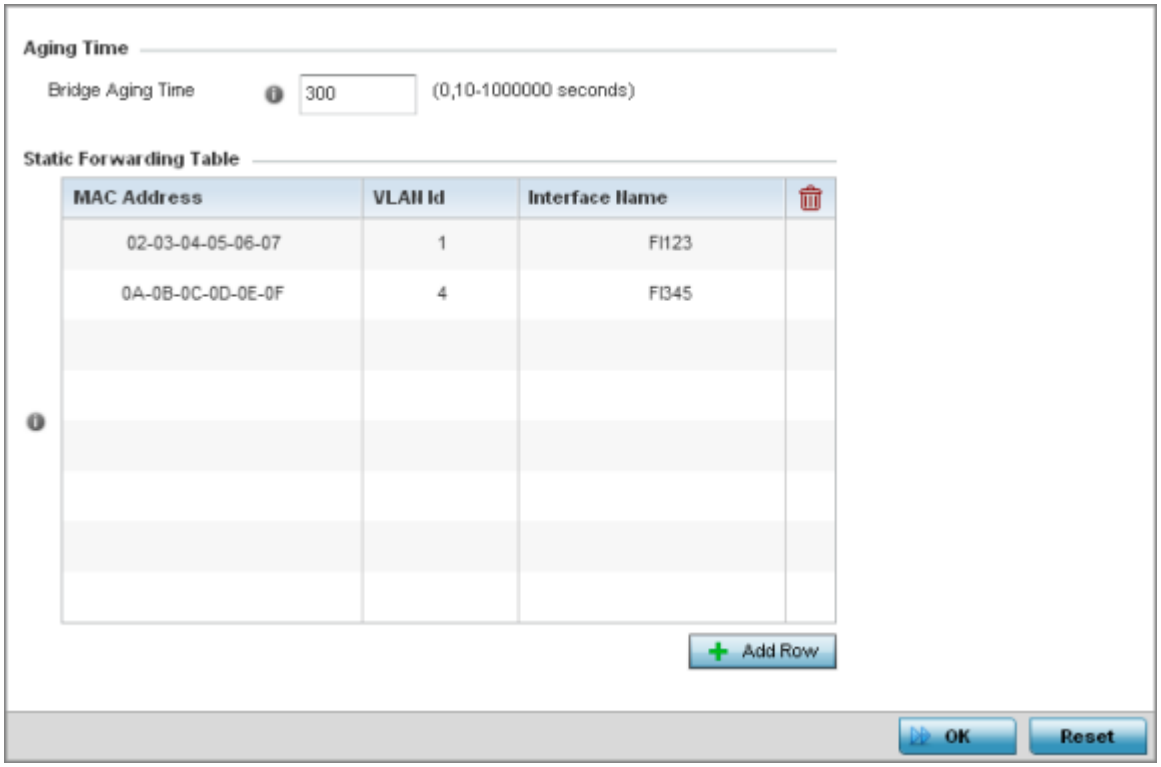



**Figure 204: Profile Overrides - Forwarding Database Configuration Screen**

4 Define a **Bridge Aging Time** from 0, 10-1,000,000 seconds.

The aging time defines the length of time an entry will remain in the bridge's forwarding table before it is deleted due to lack of activity. If an entry replenishments a destination, generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table. The default setting is 300 seconds.

5 In the Static Forwarding Table table, click **+Add Row** and define the following:

| | |
|---|---|
| MAC Address | Set or override a destination MAC Address.<br>The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). |
| VLAN ID | Define the target VLAN ID if the destination MAC is on a different network segment. |
| Interface Name | Provide the name of the interface used as the target destination interface for the target MAC address. |

6 Select **OK** to save the changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - Bridge VLAN

A VLAN *(Virtual LAN )* is separately administrated virtual network within the same physical network. VLANs are broadcast domains defined within switches to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

Note

For information, see Bridge VLAN Configuration on page 195.

To override an access point profile's Bridge VLAN configuration:

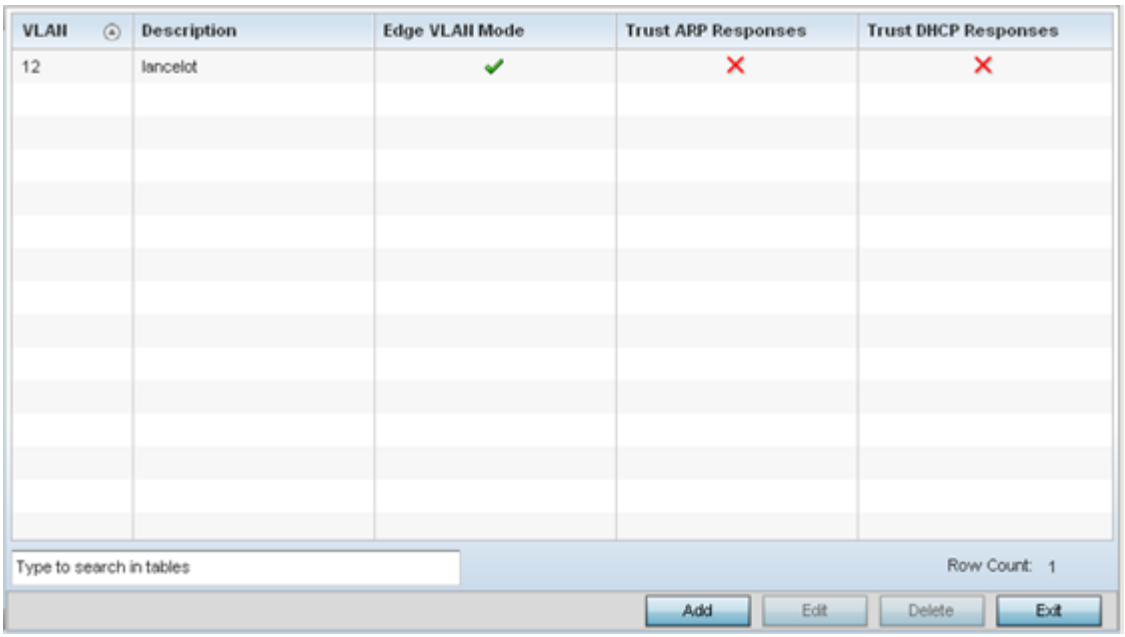
1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand the **Network** node and select **Bridge VLAN**. The Bridge VLAN Main screen displays. This screen displays existing Bridge VLAN configurations.




4 Review the following VLAN configuration parameters to determine whether an update is warranted:

| | |
|---|---|
| VLAN | Lists the numerical identifier defined for the Bridge VLAN when initially created. The available range is from 1 - 4095. This value cannot be modified during the edit process. |
| Description | Lists a description of the VLAN assigned when it was created or modified. The description should be unique to the VLAN's specific configuration and help differentiate it from other VLANs with similar configurations. |
| Edge VLAN Mode | Defines whether the VLAN is currently in edge VLAN mode. A green checkmark defines the VLAN as extended. An edge VLAN is the VLAN where hosts are connected. For example, if VLAN 10 is defined with wireless clients, and VLAN 20 is where the default gateway resides, VLAN 10 should be marked as an edge VLAN and VLAN 20 shouldn't. When defining a VLAN as an edge VLAN, the firewall enforces additional checks on hosts in that VLAN. For example, a host cannot move from an edge VLAN to another VLAN and still keep firewall flows active. |

| | |
|---|---|
| Trust ARP Response | When ARP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks. |
| Trust DHCP Responses | When DHCP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. |

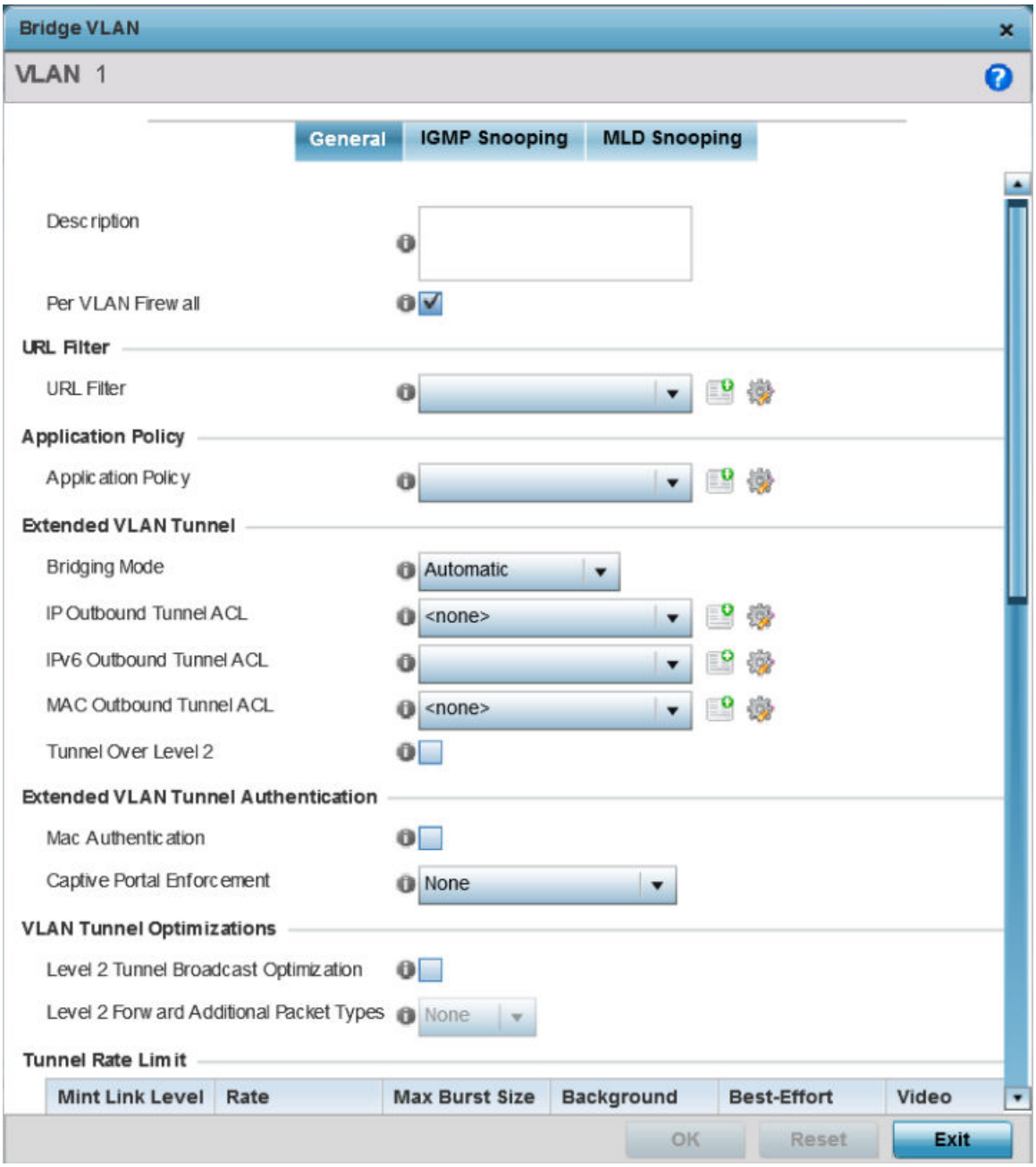
5 Select **Add** to define a new bridge VLAN configuration, **Edit** to modify an existing bridge VLAN configuration or **Delete** to remove a VLAN configuration.

Bridge VLAN General Settings

To define a bridge VLAN general configuration:

1 Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

The General tab displays by default.




2 If adding a new Bridge VLAN configuration, use the spinner control to define a **VLAN** ID between 1 - 4094. This value must be defined and saved before the General tab can become enabled and the remainder of the settings defined. VLAN IDs 0 and 4095 are reserved and unavailable.

3 Set the following general bridge VLAN parameters:

| | |
|---|---|
| Description | If creating a new Bridge VLAN, provide a description (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations. |
| Per VLAN Firewall | Enable this setting to provide firewall allow and deny conditions over the bridge VLAN. This setting is enabled by default. |

4 Set or override the following URL Filter parameters. Web filters are used to control the access to resources on the Internet:

| | |
|---|---|
| URL Filter | Use the drop-down menu to select a URL filter to use with this Bridge VLAN. |

5 Set or override the following Application Policy parameters. Use the drop-down to select the appropriate Application Policy to use with this Bridge VLAN configuration.

6 Set the following Extended VLAN Tunnel parameters:

| | |
|---|---|
| Bridging Mode | Specify one of the following bridging modes for the VLAN.<br>*Automatic*: Select automatic to let the controller, service platform or access point determine the best bridging mode for the VLAN.<br>*Local*: Select Local to use local bridging mode for bridging traffic on the VLAN.<br>*Tunnel*: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN.<br>*isolated-tunnel*: Select isolated-tunnel to use a dedicated tunnel for bridging VLAN traffic. |
| IP Outbound Tunnel ACL | Select an IP Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound IP ACL is not available, select the *Create* button to make a new one. |
| MAC Outbound Tunnel ACL | Select a MAC Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound MAC ACL is not available click the Create button to make a new one. |
| Tunnel Over Level 2 | Select this option to allow VLAN traffic to be tunneled over level 2 links. This setting is disabled by default. |

**Note**

Local and Automatic bridging modes do not work with ACLs. ACLs can only be used with tunnel or isolated-tunnel modes.

7 Set the following Extended VLAN Tunnel Authentication settings:

| | |
|---|---|
| MAC Authentication | Select to enable source MAC authentication for extended VLAN and tunneled traffic (MiNT and L2TPv3) on this bridge VLAN. When enabled, it provides fast path authentications of clients, whose captive portal session has expired. This option is disabled by default. |
| Captive-Portal Authentication | Use the drop-down menu to specify authentication mode used for extended VLAN and tunneled traffic, on this Bridge VLAN. The options are:<br>**`None`** – No Authentication mode used. This is the default setting.<br>**`Authentication Failure`** – Configures MAC Authentication as the primary and Captive-Portal Authentication as the fall-back authentication mode.<br>**`Always`** – Configures Captive-Portal Authentication as the only mode of Authentication |
| Edge VLAN Mode | Select this option to enable edge VLAN mode. When selected, the edge controller's IP address in the VLAN is not used, and is now designated to isolate devices and prevent connectivity. This feature is enabled by default. |

8 Set the following Layer 2 Firewall parameters:

| | |
|---|---|
| Trust ARP Response | Select this option to use trusted ARP packets to update the DHCP Snoop Table to prevent IP spoof and arp-cache poisoning attacks. This feature is disabled by default. |
| Trust DHCP Responses | Select this option to use DHCP packets from a DHCP server as trusted and permissible within the managed network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. This feature is disabled by default. |
| Edge VLAN Mode | Select this option to enable edge VLAN mode. When selected, the edge controller's IP address in the VLAN is not used, and is now designated to isolate devices and prevent connectivity. This feature is enabled by default. |

9 Click the **OK** button to save the changes to the General tab.

Click **Reset** to revert to the last saved configuration.

Bridge VLAN IGMP Snooping

IGMP is used for managing IP multicast group members. Controllers and service platforms listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the controller or service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

To override a device's profile bridge VLAN IGMP settings:

1 Select the **IGMP Snooping** tab.

2 Define the following General IGMP parameters:

| | |
|---|---|
| Enable IGMP Snooping | Select the check box to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the effective setting is disabled. |
| Forward Unknown Unicast Packets | Select the check box to enable to forward multicast packets from unregistered multicast groups. If disabled (the default setting), the unknown multicast forward feature is also disabled for individual VLANs. |
| Enable Fast Leave Processing | Select this option to remove a Layer 2 LAN interface from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network. |
| Last Member Query Count | Specify the number of group specific queries sent before removing an IGMP snooping entry. |

3 Within the Multicast Router section, select those interfaces used as multicast router interfaces. Multiple interfaces can be selected and overridden. Set the **`pim-dvmrp`** or **`static`** Multicast Routing Learn Mode. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths.

4 Set the following **IGMP Querier** parameters:

| | |
|---|---|
| Enable IGMP Snooping | IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server, hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port. |
| Source IP Address | Define an IP address applied as the source address in the IGMP query packet. This address is used as the default VLAN querier IP address. |
| IGMP Version | Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. The default setting is 3. |
| Maximum Response Time | Specify the maximum time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. For IGMP reports from wired ports, reports are only forwarded to the multicast router ports. The default setting is 10 seconds. |
| Other Querier Timer Expiry | Specify an interval in either **Seconds** (60 - 300) or **Minutes** (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute. |

5 Select the **OK** button to save the changes to the bridge VLAN IGMP Snooping tab.

Select **Reset** to revert to the last saved configuration.

MLD Snooping

MLD *(Multicast Listener Discovery)* snooping enables a controller, service platform or access point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or access point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To set the MLD Snooping parameters:

1 Select the **MLD Snooping** tab.

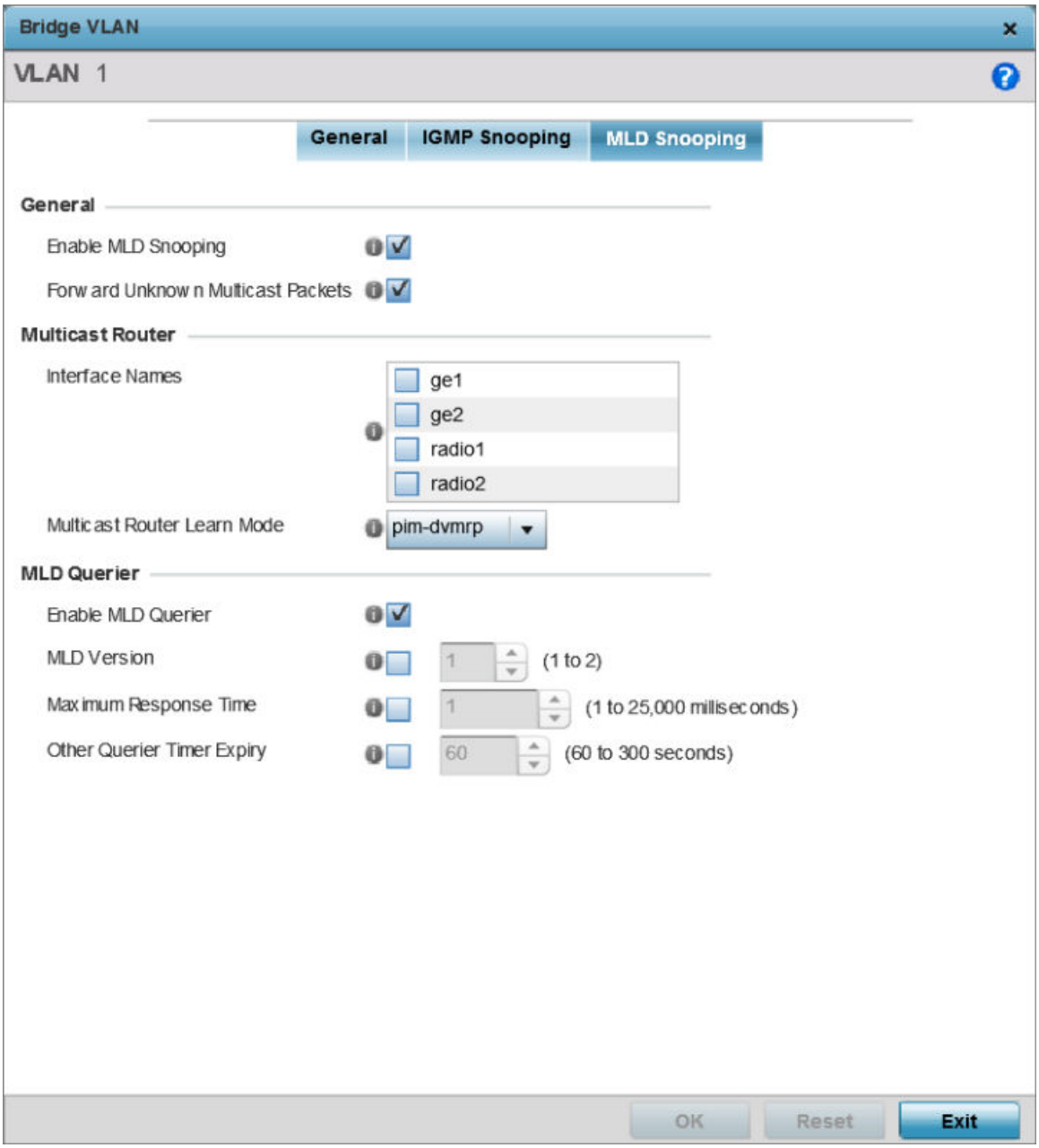



**Figure 205: Network Bridge VLAN screen, MLD Snooping tab**

2 Define the following General MLD snooping parameters for the Bridge VLAN configuration:

| | |
|---|---|
| Enable MLD Snooping | Enable MLD snooping to examine MLD packets and support content forwarding on this Bridge VLAN. Packets delivered are identified by a single multicast group address. Multicast packets are delivered using best-effort reliability, just like IPv6 unicast. MLD snooping is enabled by default. |
| Forward Unknown Packets | Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default. |

3 Define the following Multicast Router settings:

| | |
|---|---|
| Interface Names | Select the ge or radio interfaces used for MLD snooping. |
| Multicast Router Learn Mode | Set the pim-dvmrp or static multicast routing learn mode. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths. |

4 Set the following MLD Querier parameters for the profile's Bridge VLAN configuration:

| | |
|---|---|
| Enable MLD Querier | Select this option to enable MLD querier on the controller, service platform or access point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is enabled by default. |
| MLD Version | Define whether MLD version 1 or 2 is utilized with the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2. |
| Maximum Response Time | Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 1 milliseconds. |
| Other Querier Timer Expiry | Specify an interval in either Seconds (60 - 300) or Minutes (1 - 5) used as a timeout interval for other querier resources. The default setting is 60 seconds. |

5 Click the **OK** button located at the bottom right of the screen to save the changes.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - CDP

The CDP *(Cisco Discovery Protocol)* is a proprietary Data Link Layer protocol implemented in Cisco networking equipment. It's primarily used to obtain IP addresses of neighboring devices and discover their platform information. CDP is also used to obtain information about the interfaces the access point uses. CDP runs only over the data link layer enabling two systems that support different network-layer protocols to learn about each other.

To override an access point profile's CDP configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **Cisco Discovery Protocol (CDP)**.

The CDP configuration screen displays.

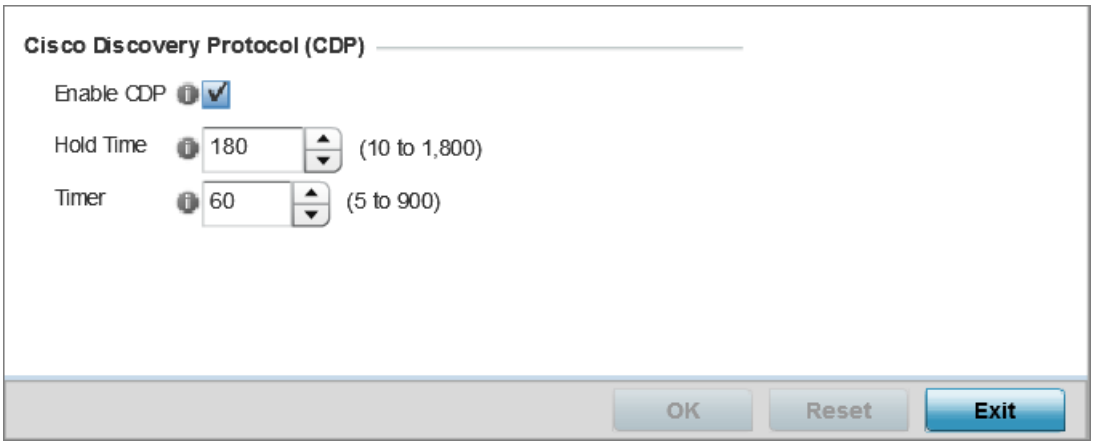



**Figure 206: Profile Overrides - Network - CDP Comfiguration Screen**

4 Select the Enable CDP option, and set the following parameters:

| | |
|---|---|
| Hold Time | Set a hold time (in seconds) for the transmission of CDP packets. Set a value from 10 - 1,800. The default setting is 180 seconds. |
| Timer | Use the spinner control to set the interval for CDP packet transmissions. The default setting is 60 seconds. |

5 Select the **OK** button to save the CDP configuration changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - LLDP

The LLDP *(Link Layer Discovery Protocol)* provides a standard way for a controller or access point to advertise information about themselves to networked neighbors and store information they discover from their peers.

LLDP is neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about them to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management and connection endpoint information from adjacent devices.

Using LLDP, an access point is able to advertise its own identification, capabilities and media-specific configuration information and learn the same information from connected peer devices.

LLDP information is sent in an Ethernet frame at a fixed interval. Each frame contains one m LLDP PDU*(Link Layer Discovery Protocol Data Unit)*. A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

To override the access point profile's LLDP configuration:

1 Go to **Configuration** → **Devices** → **Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides → Network** and select **Link Layer Discovery Protocol (LLDP)**.

The LLDP configuration screen displays.

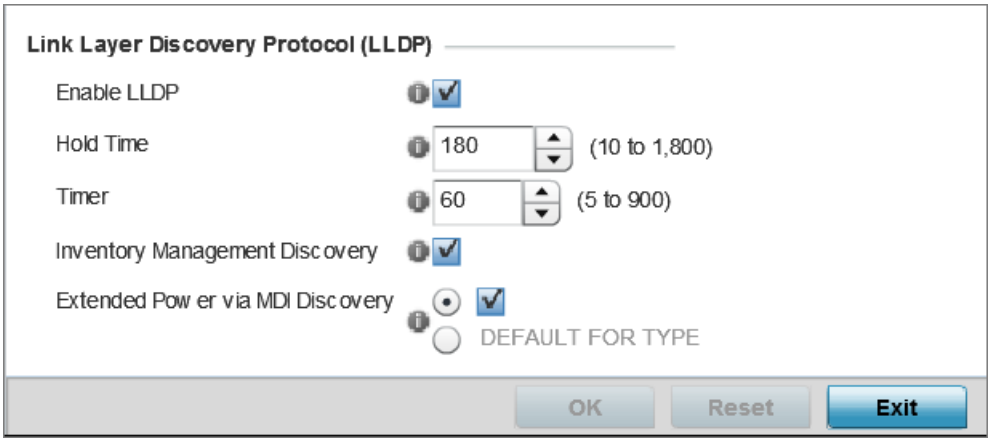



**Figure 207: Profile Overrides - Network - LLDP Configuration Screen**

4 Select the **Enable LLDP** option, and set the following parameters:

| | |
|---|---|
| Hold Time | Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value from 10 - 1,800. The default hold time is 180 seconds. |
| Timer | Set the interval used to transmit LLDP PDUs. Define an interval from 5 - 900 seconds. The default setting is 60 seconds. |
| Inventory Management Discovery | Select this option to include LLPD-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default. |
| Extended Power via MDI Discovery | Select this option to include LLPD-MED *(LLDP - Media Endpoint Discovery)* extended power via MDI *(Media Dependent Interface)* discovery TLV in LLDP PDUs. This setting is disabled by default. |

5 Select **OK** to save the LLDP configuration changes.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - Miscellaneous

An access point profile can include a hostname within a DHCP lease for a requesting device. This helps an administrator track the leased DHCP IP address by hostname for the supported device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices. At the device level, this setting can be overridden.

To override an access point profile's miscellaneous settings:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **Miscellaneous**.

The miscellaneous configuration screen displays.

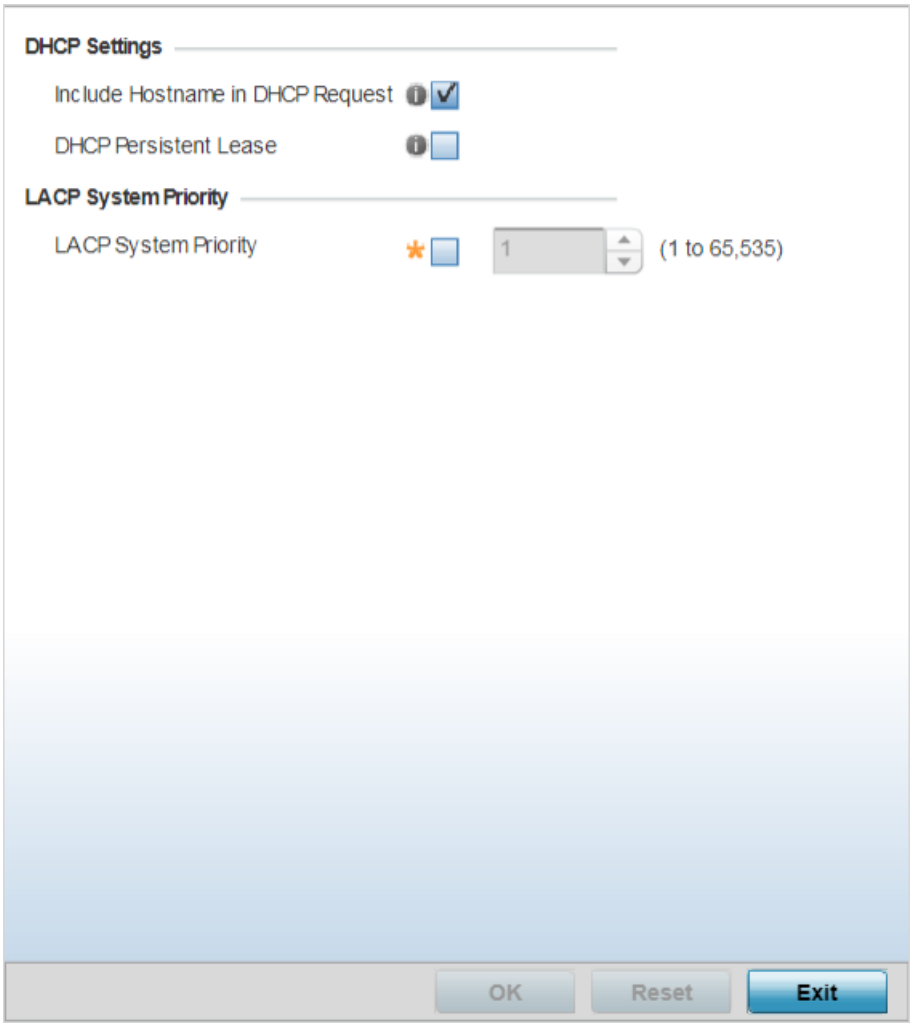



**Figure 208: Profile Overrides - Network - Miscellaneous Configuration Screen**

4 In the DHCP Settings field, set the following parameters:

| | |
|---|---|
| Include Hostname in DHCP Request | Select to enable the inclusion of hostname in a DHCP lease for a requesting device. This feature is enabled by default. |
| DHCP Persistent Lease | Select to enable retention of the last-used lease (used by the access point) if the access point's DHCP server resource were to become unavailable. This feature is enabled by default. |

5 In the LACP System Priority field, select the **LACP System Priority** option and use the associated spinner control to set this access point's priority in the LACP negotiation process.

Use to configure an LACP-enabled peer's system priority value. LACP *(Link Aggregation Control Protocol)* uses this system priority value along with the peer's MAC address to form the system ID. In a LAG *(Link Aggregation Group)*, the peer with the lower system ID initiates LACP negotiations with another peer. In scenarios, where both peers have the same system-priority value assigned, the peer with the lower MAC gets precedence.

6 Select **OK** to save the miscellaneous configuration changes.

Select **Reset** to revert to the last saved configuration.

### Aliases Overview

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- Global aliases are defined from the **Configuration → Network → Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- Profiles aliases are defined from **Configuration → Devices → System Profile → Network → Alias**. These aliases are available for use to a specific group of wireless controllers or access points. Alias values defined in this profile override alias values defined within global aliases.
- RF Domain aliases are defined from **Configuration → Devices → RF Domain →Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- Device aliases are defined from **Configuration → Devices → Device Overrides → Network → Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an Network Alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the Network Alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the Network Alias works with the 172.16.10.0/24 network. Existing ACLs using this Network Alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Aliases can be classified as:

- Basic Alias
- Network Group Alias
- Network Service Alias

Network Basic Alias

A *basic alias* is a set of configurations consisting of *VLAN*, *Host*, *Network*, *Address Range*, and *String* alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

To set a network basic alias configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network. Select a target access point.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides → Network** and select **Alias**.

The Basic Alias screen displays.

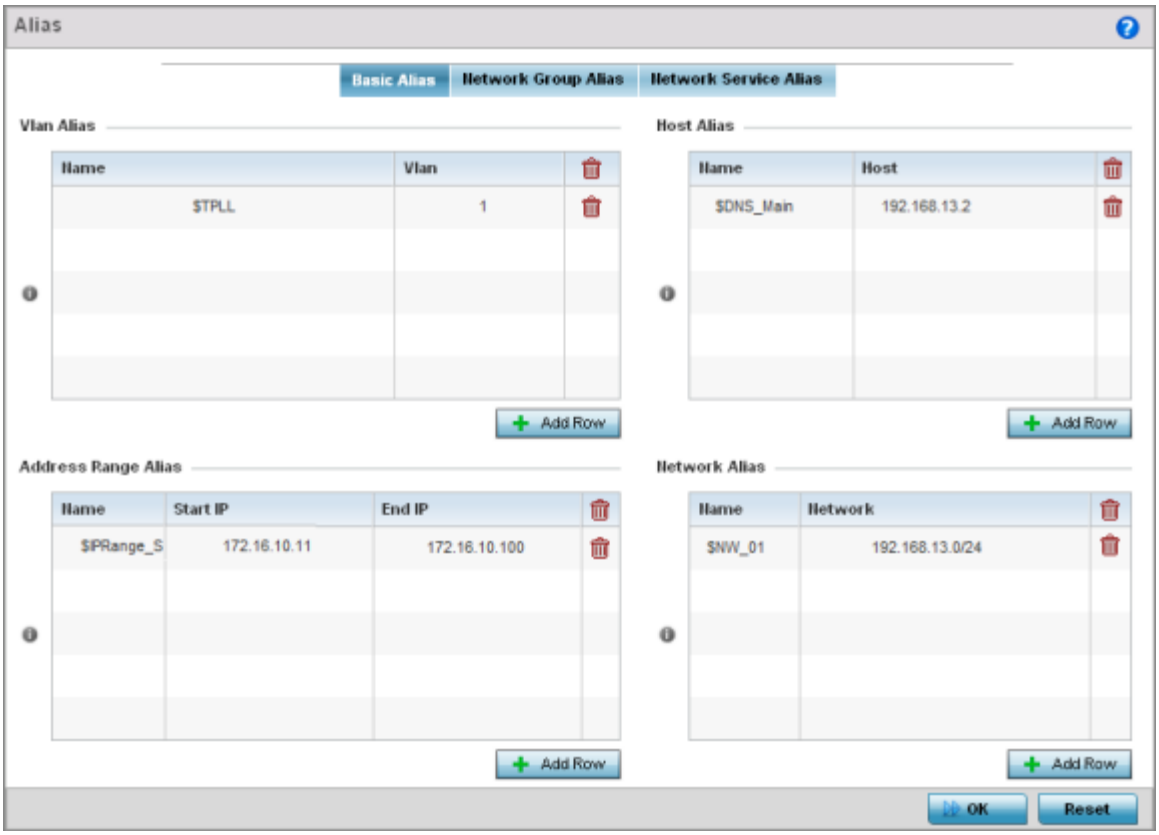



**Figure 209: Network - Basic Alias Screen**

4 Select **+ Add Row**, in the VLAN Alias table to add a VLAN alias settings.

VLANs aliases can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

| | |
|---|---|
| Name | If adding a new VLAN Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| VLAN | Use the spinner control to set a numeric VLAN from 1 - 4094. |

5 Select **+ Add Row**, in the Address Range Alias table to add an address range alias settings.

This option creates an alias for a range of IP address that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

| | |
|---|---|
| Name | If adding a new Address Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Start IP | Set a starting IP address used with a range of addresses utilized with the address range alias. |
| End IP | Set a ending IP address used with a range of addresses utilized with the address range alias. |

**Note**

An address range alias can be used to replace an IP address range in IP firewall rules.

6 Select **+ Add Row**, in the Host Alias table to add a host alias settings:

This option creates aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new Host Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Host | Set the IP address of the host machine. |

7 Select **+ Add Row**, in the Network Alias table to add a network alias settings:

This option create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new Network Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Network | Provide a network address in the form of host/mask. |

8 Select **+ Add Row**, in the String Alias table to add a string alias settings:

This option creates aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but

remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

| | |
|---|---|
| Name | If adding a new String Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Value | Provide a string value to use in the alias. |

**Note**

A string alias can be used to replace domain name stings in DHCP.

9 Select **OK** when completed to update the basic alias rules.

Select **Reset** to revert the screen back to its last saved configuration.

Network Group Alias

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

A network group alias can be used in IP firewall rules to substitute hosts, subnets and IP address ranges.

1 Select the **Network Group Alias** tab.

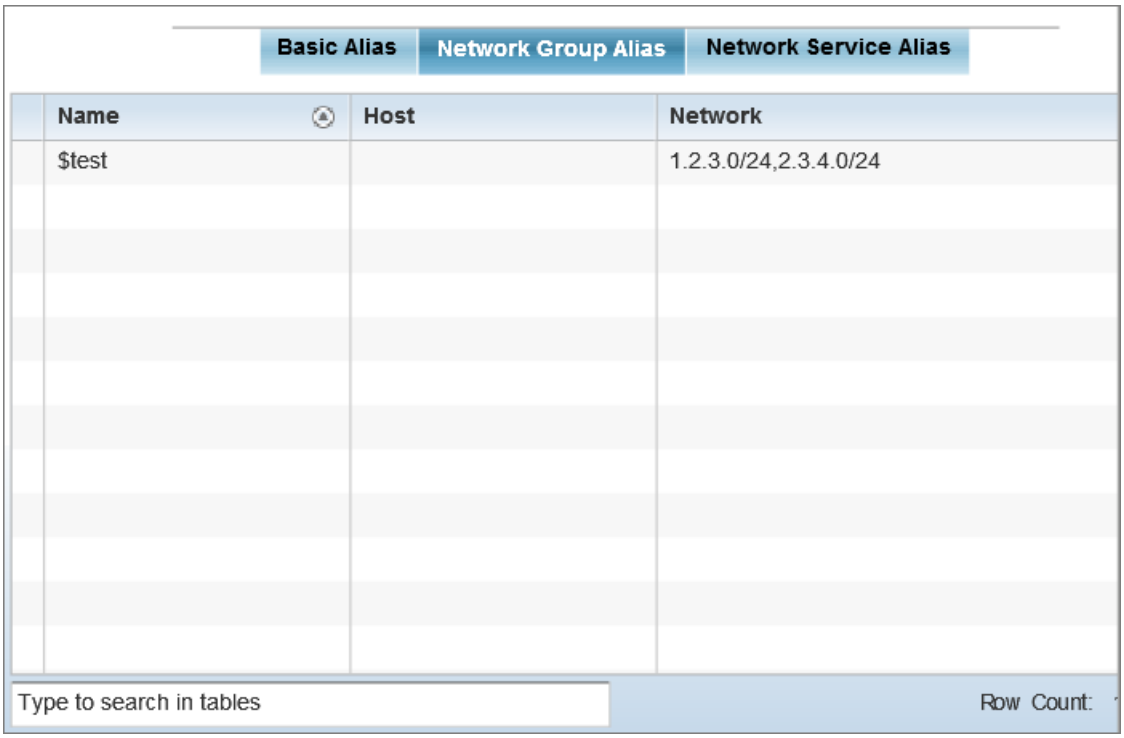



**Figure 210: Network Alias - Network Group Alias Screen**

2 Review the following to determine if a new alias configuration is needed or an existing configuration warrants modification:

| | |
|---|---|
| Name | Displays the administrator assigned name associated with the network group alias. |
| Host | Displays all the host aliases in the listed network group alias. Displays a blank column if no host alias is defined. |
| Network | Displays all network aliases in the listed network group alias. Displays a blank column if no network alias is defined. |

Adding and Editing Network Group Alias

You can add a new network group alias configuration or edit an existing configuration.

1 Select **Add** to create a new alias, **Edit** to modify the attributes of an existing alias, or **Delete** to remove obsolete aliases.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

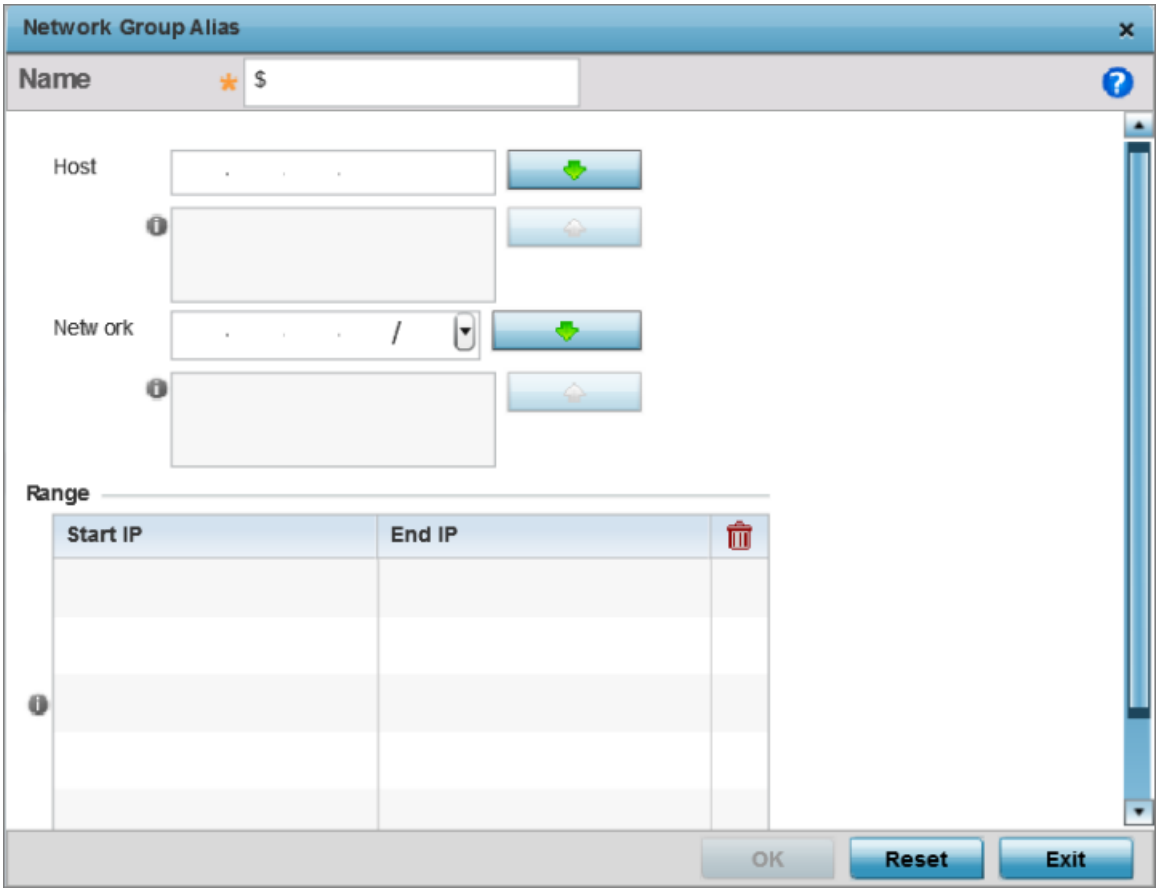



**Figure 211: Network Alias - Network Group Alias Add Screen**

2 If you are adding a new network alias rule, provide a `name` up to 32 characters. The network group alias name always starts with a dollar sign ($).

3 Define the following network group alias parameters:

| | |
|---|---|
| Host | Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table. |
| Network | Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table. |

4 Select **+ Add Row**, in the Range table to specify the Start IP address and End IP address for the alias range, or double-click on an existing alias range entry to edit it.

5 Select **OK** when completed to update the network group alias settings.

Select **Reset** to revert the screen to its last saved configuration.p

Network Service Alias

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to two source port ranges and up to two destination port ranges can be configured. A maximum of four protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

A network service alias can be used to substitute protocols and ports in IP firewall rules.

Select the **Network Service Alias** tab.

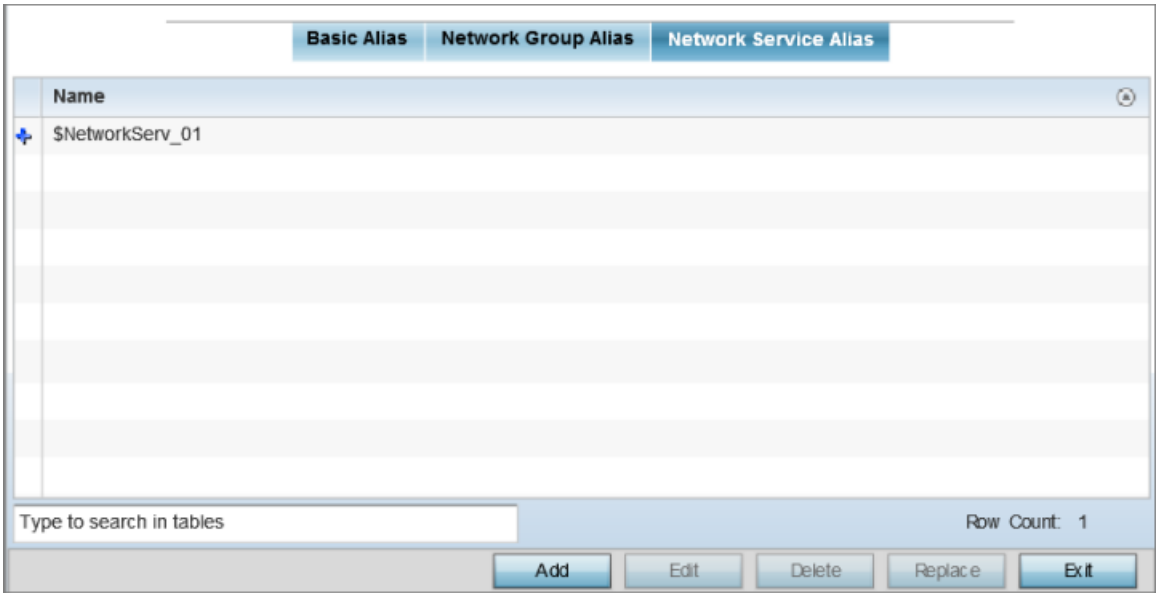



**Figure 212: Network Alias - Network Service Alias Screen**

Adding and Editing Network Service Alias

You can add a new network service alias configuration or edit an existing configuration.

1 Select **Add** to create a new network service alias.

Select an existing network service alias and click **Edit** to modify it. Select **Delete** to remove an existing network service alias from those available in the list.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

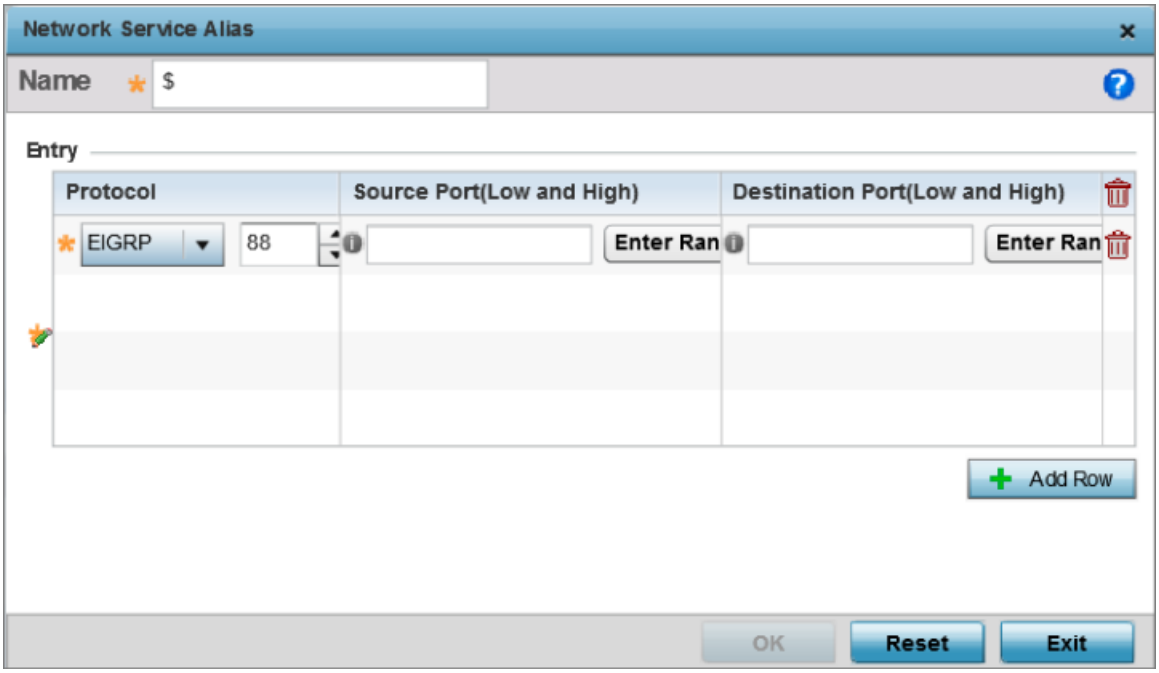



**Figure 213: Network Alias - Network Service Alias Add screen**

2 If you are adding a new Network Service Alias, give it a `Name` up to 32 characters to distinguish this alias configuration from others with similar attributes.

Note

The Network Service Alias name always starts with a dollar sign ($).

3 Select **+ Add Row**, in the Entry table and specify the following parameters:

| | |
|---|---|
| Protocol | Specify the protocol for which the alias is created. Use the drop down to select the protocol from **`eigrp`**, **`gre`**, **`icmp`**, **`igmp`**, **`ip`**, **`vrrp`**, **`igp`**, **`ospf`**, **`tcp`** and **`udp`**. Select **`other`** if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected. |
| Source Port (Low and High) | This field is relevant only if the protocol is *tcp* or *udp*.<br>Specify the source ports for this protocol entry. A range of ports can be specified. Select the **Enter Range** button next to the field to enter a lower and higher port range value. Up to eight (8) ranges can be specified. |
| Destination Port (Low and High) | This field is relevant only if the protocol is *tcp* or *udp*.<br>Specify the destination ports for this protocol entry. A range of ports can be specified. Select the **Enter Range** button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified. |

4 Select **OK** when completed to update the network service alias rules.

Select **Reset** to revert the screen back to its last saved configuration.

Aliases - Encrypted String

An encrypted string alias maps a user-friendly name to a string value. The string value displays as encrypted text when "password-encryption" is enabled. Encrypted-string aliases can be used for string configuration parameters that are encrypted by the "password-encryption" feature.

To configure an encrypted string alias on an access point:

1 Select the **Encrypted String** alias tab.

The encrypted string alias configuration screen displays.

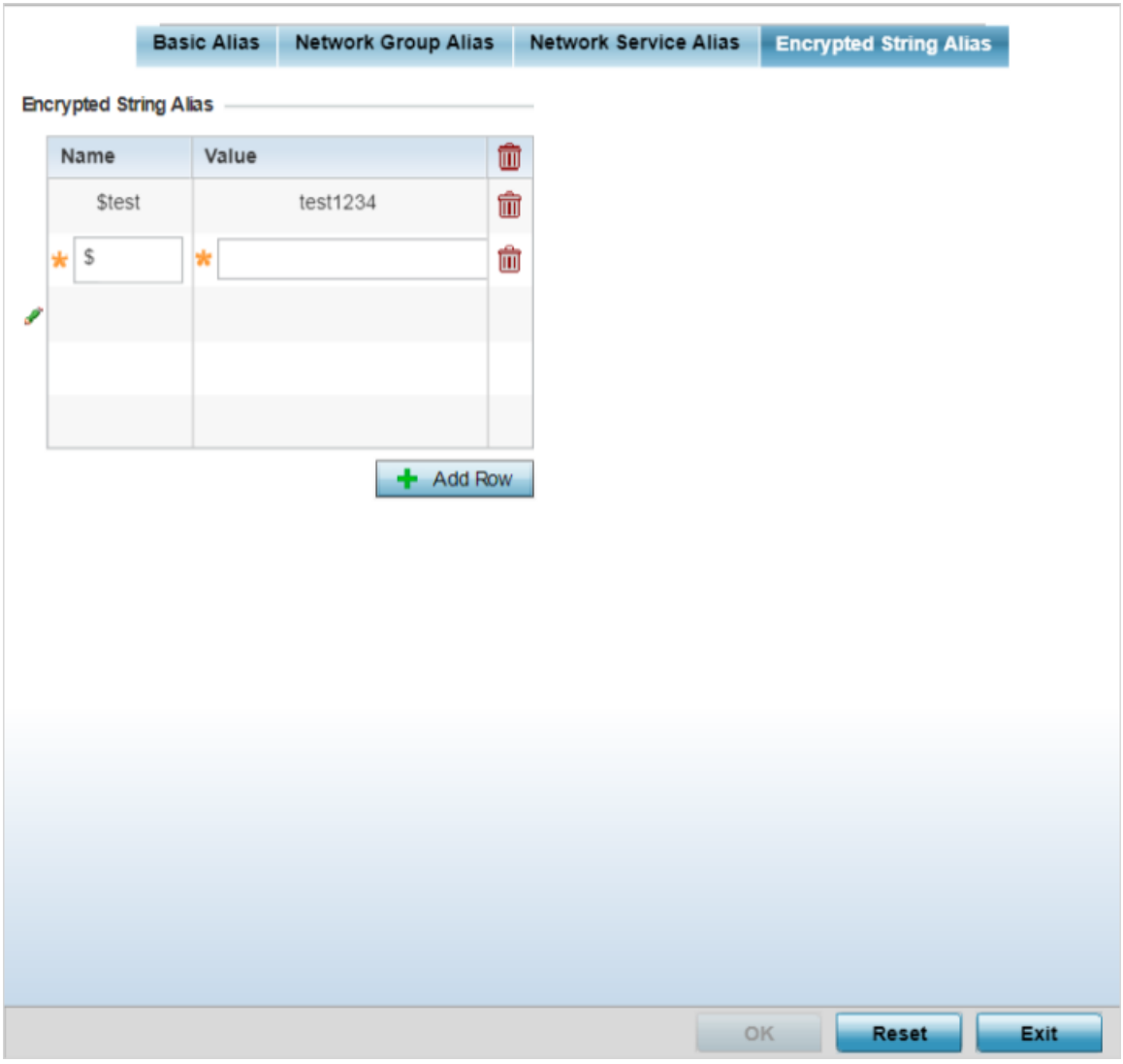



**Figure 214: Profile Overrides - Encrypted String Alias Configuration Screen**

2 In the Encrypted String Alias table, click **+ Add Row** and set the following parameters:

| | |
|---|---|
| Name | Provide a `name` for the encrypted string alias.<br><br>Note:<br>The alias name should start with a dollar sign ($), and not exceed 32 characters in length. |
| Value | Enter the string value associated with the alias name provides above. |

3 Select **OK** when completed to update the encrypted string alias rules.

Select **Reset** to revert the screen back to its last saved configuration.

### Profile Overrides - IPv6 Neighbors

IPv6 neighbor discovery uses ICMP messages and solicited multicast addresses to find the link layer address of a neighbor on the same local network, verify the neighbor's reachability and track neighboring devices.

Note

For more information on IPv6 neighbor discovery, see Profile Overrides - IPv6 Neighbors on page 463.

At the device level, you can override the device profile's IPv6 neighbor settings. To override the access point Profile's IPv6 neighbor configurations:

1 Go to **Configuration** → **Devices** → **Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **IPv6 Neighbor**.

The IPv6 neighbor configuration screen displays.

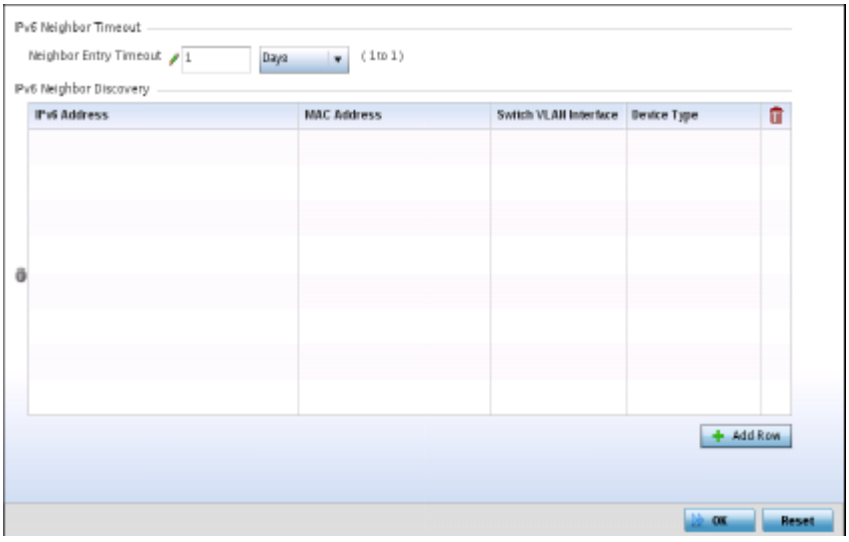



**Figure 215: Profile Overrides - Network - IPv6 Neighbor Configuration Screen**

4 In the IPv6 Neighbor Timeout field, set the **IPv6 Neighbor Entry Timeout** in either Seconds (15 - 86,400), Minutes (1 - 1,440), Hours (1 - 24) or Days (1). The default setting is 1 hour.

5 In the IPv6 Neighbor Discovery table, click **+ Add Row** and set the following parameters:

| | |
|---|---|
| IPv6 Address | Provide a static IPv6 IP address for neighbor discovery. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the Neighbor Discovery Protocol via ICMPv6 *(Internet Control Message Protocol version 6)* router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| MAC Address | Enter the hardware encoded MAC addresses of up to 256 IPv6 neighbor devices. A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable. |
| Switch VLAN Interface | Use the spinner control to set the virtual interface (from 1 - 4094) used for neighbor advertisements and solicitation messages. |
| Device Type | Specify the device type for this neighbor solicitation is for. Options include: **`Host`**, **`Router`** and **`DHCP Server`**. The default setting is *Host*. |

6 Select **OK** to save the IPv6 neighbor configuration changes.

Select **Reset** to revert to the last saved configuration.

*Profile Overrides - Security*

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy applied. If an existing firewall, client role or NAT policy is unavailable create the required security policy configuration. Once created, a configuration can have an override applied as needed to meet the changing data protection requirements of a device's deployed environment. However, in doing so this device must now be managed separately from the profile configuration shared by other identical models within the network.

For more information on applying an override to an existing device profile, refer to the following sections:

- Profile Overrides - VPN on page 464
- Profile Overrides - Auto IPSec Tunnel on page 474
- Profile Overrides - Settings on page 476
- Profile Overrides - Certificate Revocation on page 478
- Profile Overrides - Trustpoints on page 479
- Profile Overrides - NAT Pool on page 481
- Profile Overrides - Bridge NAT on page 491
- Profile Overrides - Application Visibility (AVC) on page 494

### Profile Overrides - VPN

VPN can be overridden by using either the inbuilt wizards or by manually configuring the required parameters. This section describes how to use the inbuilt wizards to override the VPN parameters. The user interface provides two (2) wizards that provide different levels of configuration.

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides → Security** and select **VPN**.

The selected access point's Security configuration screen displays, with the VPN option selected by default.

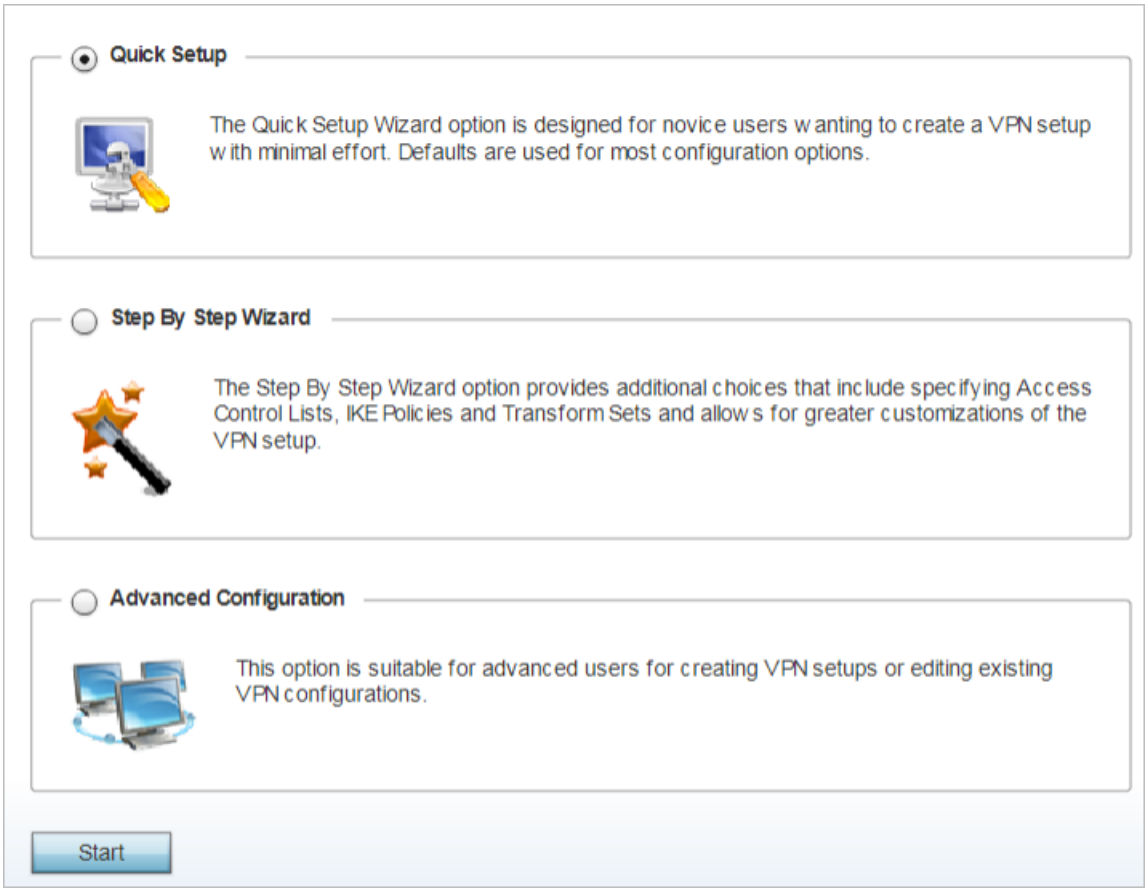



**Figure 216: Profile Overrides - Security - VPN Configuration Screen**

The following options are available:

- Quick Setup - Use this wizard to setup basic VPN Tunnel on the device. This wizard is aimed at novice users and enables them to setup a basic VPN with minimum effort. This wizard uses default values for most of the parameters.

  Note

  This option is selected by default. If you wish to use any of the other options on this screen, select the option and click **Start**.

- Step-by-Step wizard - Use this wizard to setup a VPN Tunnel step by step. This wizard is aimed at intermediate users who require the ability to customize some of the parameters.
- Advanced Configuration - Use this option to configure the VPN parameters manually.

4 Click **Start** to launch the Quick Setup wizard.
The Quick Setup wizard creates a VPN connection with minimum manual configuration. Default values are retained for most of the parameters.

The quick setup screen displays.

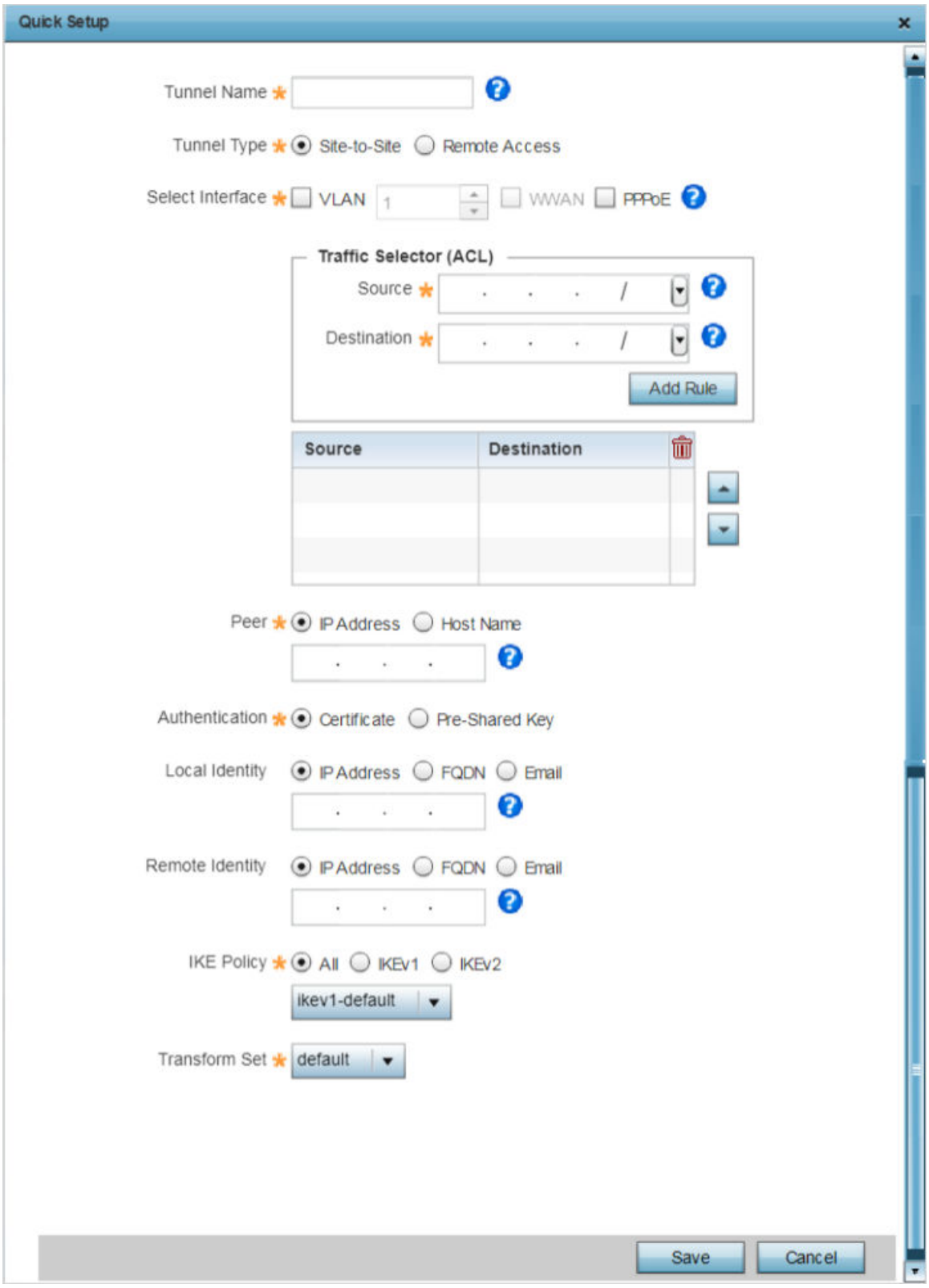



**Figure 217: VPN Quick Setup Wizard Screen**

5 Provide the following VPN tunnel configurations:

| | |
|---|---|
| Tunnel Name | Provide a name for the tunnel. Tunnel name must be such that it easily identifies the tunnel uniquely. |
| Tunnel Type | Configure the tunnel type as one of the following:<br>• **Site-to-Site** – Select to create a secured connection between two sites.<br>• **Remote Access** – Provides access to a network to remote devices. |
| Select Interface | Configure the interface for creating the tunnel. The following options are available:<br>• VLAN – Select to configure tunnel over a Virtual LAN interface. Use the spinner to configure the VLAN number.<br>• WWAN – Select to configure tunnel over the WWAN interface.<br>• PPPoE – Select to configure tunnel over the PPPoE interface |
| Traffic Selector (ACL) | Configure ACLs that manage the traffic passing through the VPN Tunnel.<br>• Source – Provide the source network along with its mask.<br>• Destination – Provide the destination network along with its mask.<br><br>Note:<br>Click **Add Rule** to add the rule into the ACL. |
| Peer | Configure the peer for this tunnel. The peer device can be specified either by its hostname or IP address. |
| Authentication | Configure the authentication used to identify peers. The options are:<br>• **Certificate** – Select to apply certificate-base peer authentication.<br>• **Pre-Shared Key** – Select to enforce pre-shared key based peer authentication. If selecting this option, provide the PSK in the associated field. |
| Local Identity | Configure the local identity used with peer configuration for an IKE exchange with the target VPN IPSec peer. Options include:<br>• **IP Address**<br>• **FQDN**<br>• **Email**<br><br>The default setting is *IP Address*. |
| Remote Identity | Configure the access point remote identifier for an IKE exchange with the target VPN IPSec peer. The options include:<br>• **IP Address**<br>• **FQDN**<br>• **Email**<br><br>The default setting is *IP Address*. |

| | |
|---|---|
| IKE Policy | Configure the IKE policy to use. IKE is used to exchange authentication keys. The options are:<br>• **All** – Select to use any IKE policy.<br>• **IKE1** – Select to only use IKE 1.<br>• **IKE2** – Select to only use IKE 2. |
| Transform Set | Configure the transform set used to specify how traffic is protected within the crypto ACL defining the traffic that needs to be protected. Select the appropriate traffic set from the drop-down menu. |

6 Click **Save** to save the VPN Tunnel configuration.

To exit without saving, click **Cancel**.

7 Select the Step-By-Step Wizard option, and click **Start** to launch the wizard.

The Step-By-Step wizard creates a VPN connection with more manual configuration than the Quick Setup Wizard. Use this wizard to manually configure Access Control Lists, IKE Policy, and Transform Sets to customize the VPN Tunnel.

The **Step-by-Step wizard** → **Basic Configuration** (step 1/4) screen displays by default.

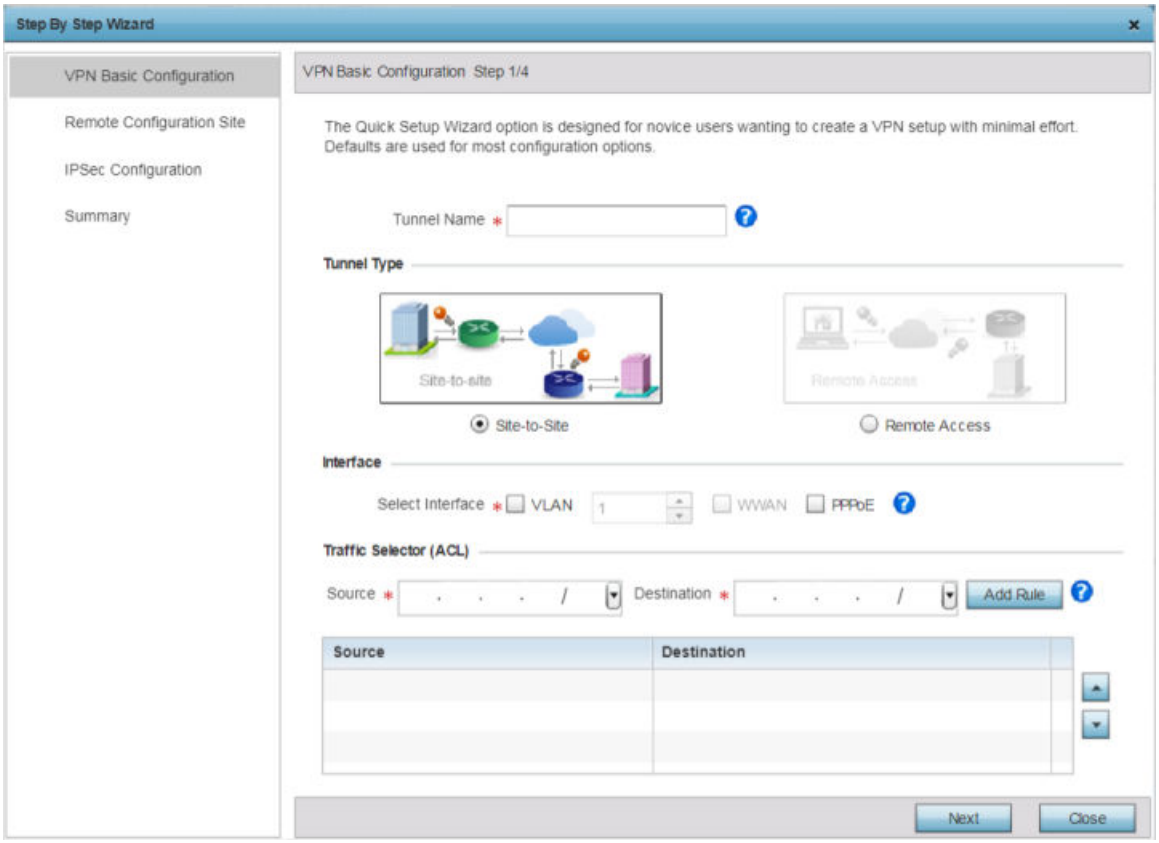



**Figure 218: VPN Basic Configuration Screen Step 1/4**

8 Provide the following basic configurations:

| | |
|---|---|
| Tunnel Name | Provide a name for the tunnel. Tunnel name must be such that it easily identifies the tunnel uniquely. |
| Tunnel Type | Configure the tunnel type as one of the following:<br>• **Site-to-Site** – Select to create a secured connection between two remote sites.<br>• **Remote Access** – Select to create a tunnel between an user device and a network. In other words, select to provide access to a network to remote devices. |
| Interface | Configure the interface for the tunnel. The options are:<br>• VLAN – Select to configure tunnel over a Virtual LAN interface. Use the spinner to configure the VLAN number.<br>• WWAN – Select to configure tunnel over the WWAN interface.<br>• PPPoE – Select to configure tunnel over the PPPoE interface |
| Traffic Selector (ACL) | This field creates the Access Control List (ACL) that is used to control who uses the network.<br>• Source – Provide the source network IP address along with its mask.<br>• Destination – Provide the destination network IP address along with its mask.<br><br>Note:<br>Click **Add Rule** to add the rule into the ACL. |

9 Click **Next**.

The **Step-by-Step Wizard → Remote Configuration Site** (step 2/4) screen displays.

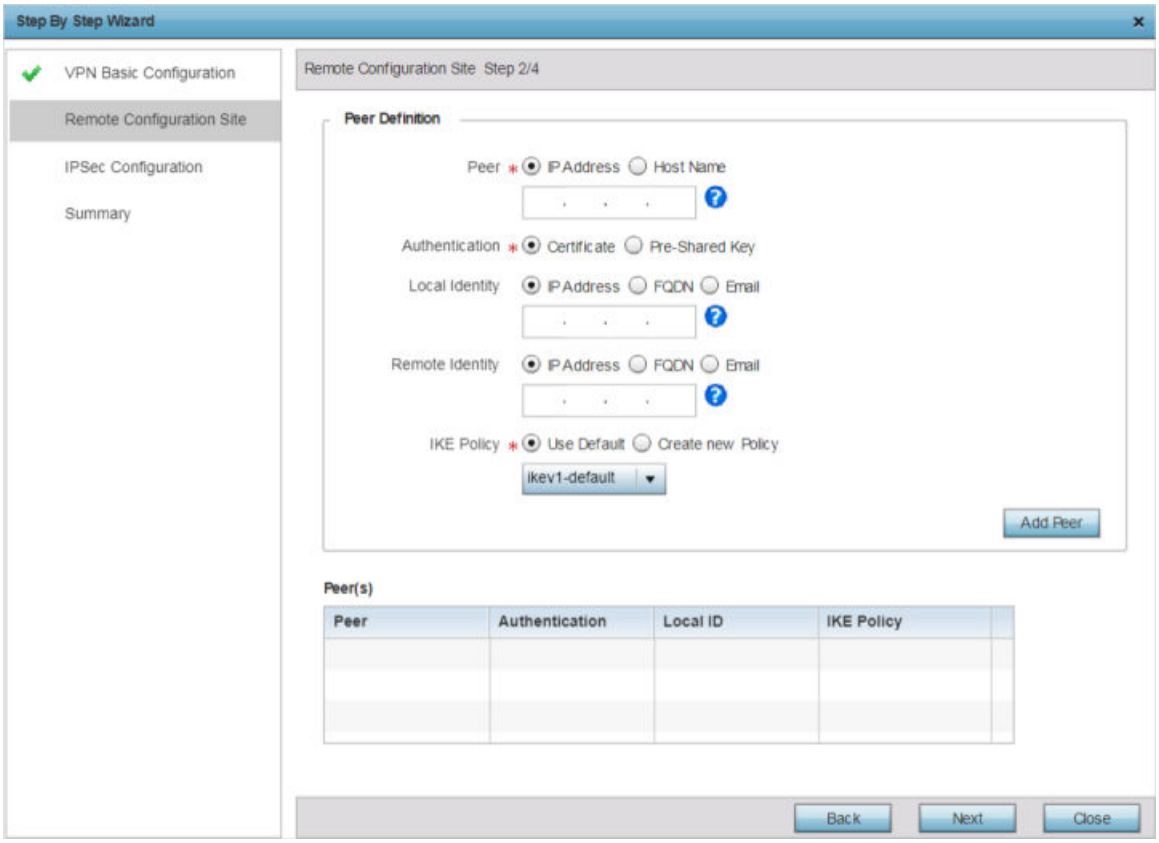



**Figure 219: Remote Configuration Site Step 2/4 Screen**

10 Provide the following remote site configuration:

| | |
|---|---|
| Peer | Specify the peer for this device when forming a tunnel. The peer can be identified by it's IP address or hostname.<br>• **`IP Address`** - Select and specify the peer's IP address in the associated field.<br>• **`Host Name`** - Select and specify the peer's hostname in the associated field. |
| Authentication | Configure the mode of authentication used by the tunnel peers. The options are:<br>• **`Certificate`** – Select to apply certificate-base peer authentication.<br>• **`Pre-Shared Key`** – Select to enforce pre-shared key based peer authentication. If selecting this option, provide the PSK in the associated field. |

| | |
|---|---|
| Local Identity | Configure the local identity used with peer configuration for an IKE exchange with the target VPN IPSec peer. Options include:<br>• **IP Address**<br>• **FQDN**<br>• **Email**<br>The default setting is *IP Address*. |
| Remote Identity | Configure the access point remote identifier for an IKE exchange with the target VPN IPSec peer. The options include:<br>• **IP Address**<br>• **FQDN**<br>• **Email**<br>The default setting is *IP Address*. |
| IKE Policy | Configure the IKE policy to use when creating this VPN Tunnel. The following options are available:<br>• **Use Default** – Select this option to use the default IKE profiles. Select one of ike1-default or ike2-default.<br>• **Create new Policy** – Select this option to create a new IKE policy. Select and click Create new Policy button to launch the IKE Policy creation window.<br>The default setting is *IP Address*. |

11 Click the **Add Peer** button to move the tunnel peer information into the Peer(s) table. This table lists all the peers configured for the VPN Tunnel.

12 Click **Next**.

The **Step-by-Step Wizard → IPSec Configuration** (step 3/4) screen displays.

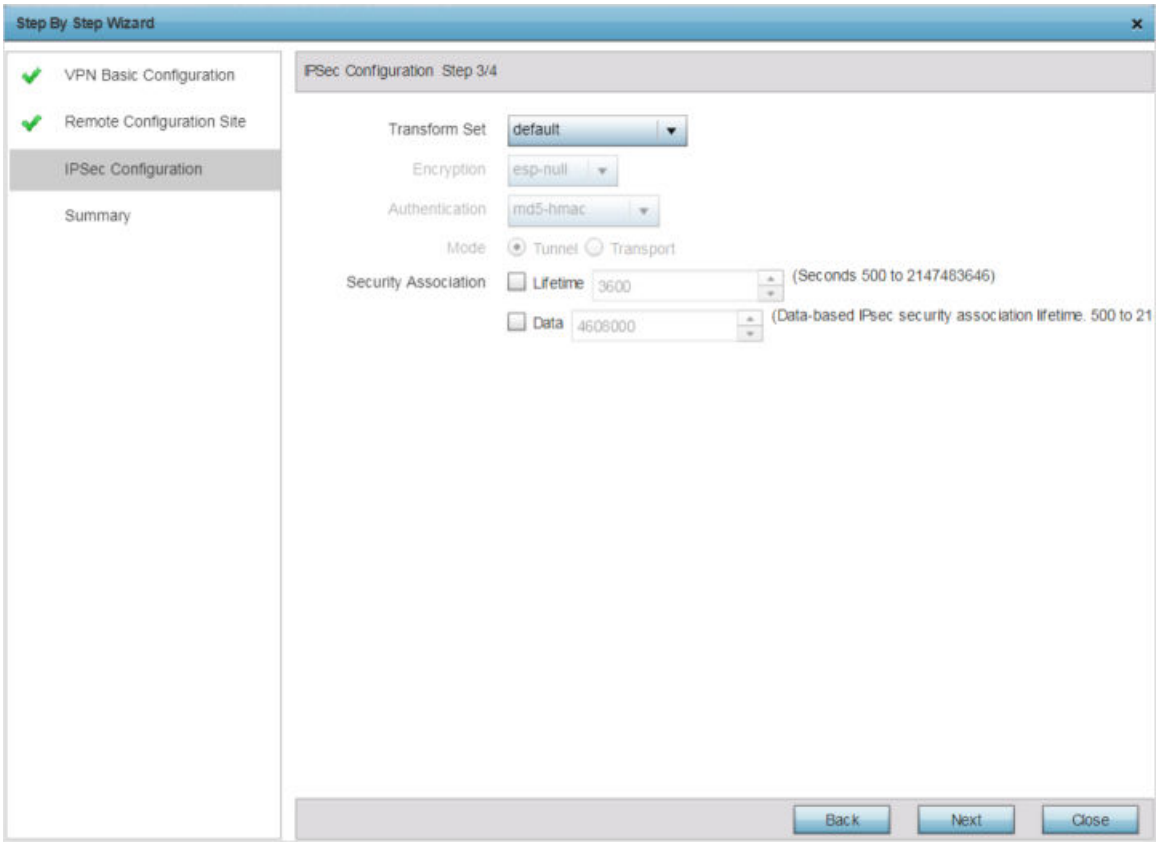



**Figure 220: IPSec Configuration Step 3/4 Screen**

13 Provide the following configurations:

| | |
|---|---|
| Transform Set | Transform set is a set of configurations exchanged for creating the VPN tunnel and impose a security policy. Use the Transform Set drop-down menu and select one of the following options:<br>• **default** - Select to apply the default, system-provided security policy.<br>• **Create New Policy** - Select to create new security policies. when selected the Encryption, Authentication and Mode fields are enabled.<br>• Authentication – The authentication used to identify tunnel peers.<br>• Mode – The mode of the tunnel. This is how the tunnel will operate.<br>Note: |
| Encryption | Specify the encryption mode used with the tunnel. The options are:<br>• **esp-null**<br>• **des**<br>• **3des**<br>• **aes**<br>• **aes-192**<br>• **aes-256** |
| Authentication | Specify the authentication mode used to identify tunnel peers. the options are:<br>• **md5-hmac**<br>• **sha-hmac**<br>• **sha256-hmac**<br>• **aes-xcbc-mac**<br>This is the method peers authenticate with as the source of the packet to other peers after a VPN Tunnel has been created. |
| Mode | Configure the mode of transport used to transmit packets through the tunnel. The options are:<br>• Tunnel – Select this mode when the tunnel is between two routers or servers.<br>• Transport – Select this mode when the tunnel is created between a client and a server. |
| Security Association | Configure the lifetime of a SA *(security association)*. Keys and SAs should be periodically renewed to maintain security of the tunnel.<br>• Lifetime – Duration in seconds after which the keys should be changed. Set a value in from 500 - 2,147,483,646 seconds. The default value is 3,600 seconds.<br>• Data – Select this option to enable data-based IPSec security association. Provide the data threshold for determining the need of Key change. The key is changed after this quantity of data has been encrypted/ decrypted. Set a value from 500 - 2,147,483,646 KBs. |

14 Click **Next**.

The **Step-by-Step Wizard → Summary** (step 4/4) screen displays.

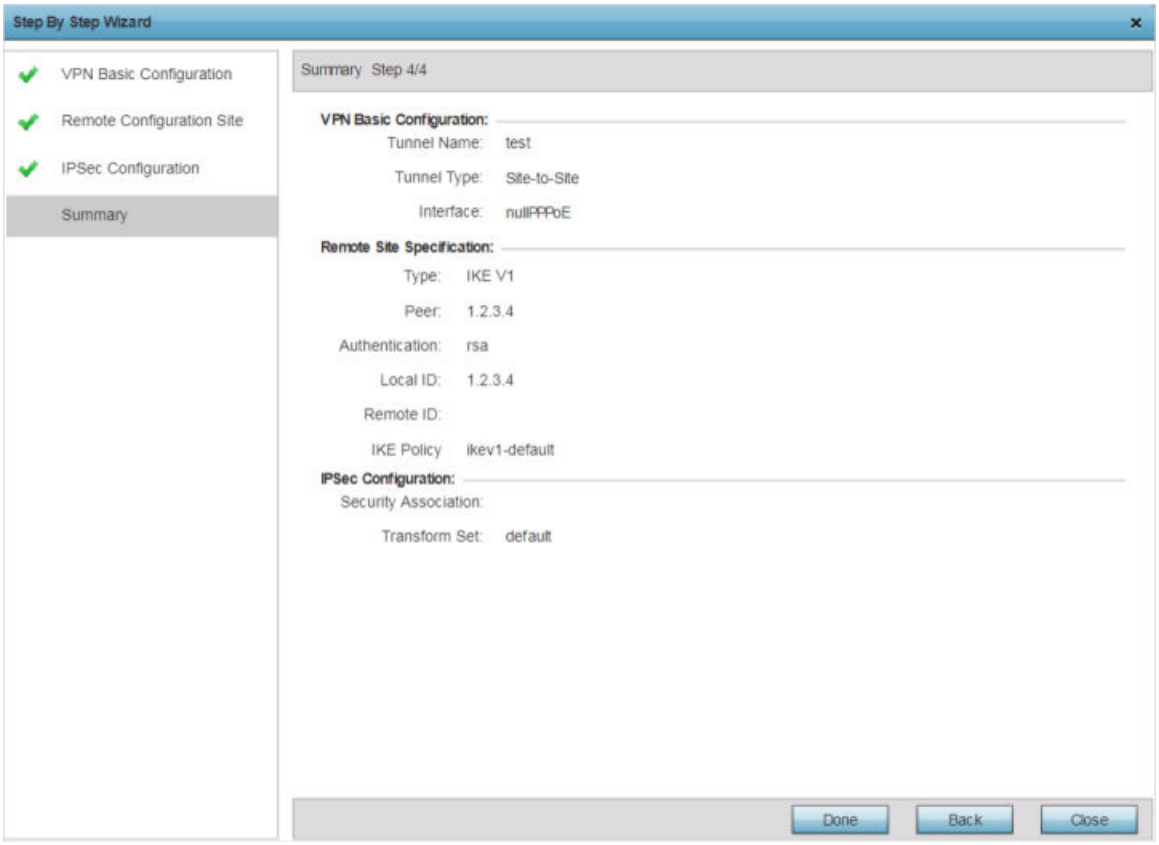



**Figure 221: Summary Step 4/4 Screen**

15 Review the configuration and click **Done** to create the VPN tunnel.

Use the **Back** button to go back to previous screen for making modifications to the configuration. Click **Close** to close the wizard without creating a VPN Tunnel.

16 Select the Advanced Configuration option, to configure the VPN parameters manually.

For detailed information manually configuring the VPN configurations, see Defining Profile VPN Settings on page 217.

### Profile Overrides - Auto IPSec Tunnel

IPSec tunnels are established to secure traffic, data and management traffic, from access points to remote wireless controllers. Secure tunnels must be established between access points and the wireless controller with minimum configuration pushed through DHCP option settings.

Note
WiNG 7.1 release does not support L2TPv3 tunneling on AAP505i and AP510i model access points. This feature will be supported in future releases.

To override profile's Auto IPSec Tunnel configuration:

1 Go to **Configuration** → **Devices** → **Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Security** and select **Auto IPSec Tunnel**.

The Auto IPSec Tunnel configuration screen displays.

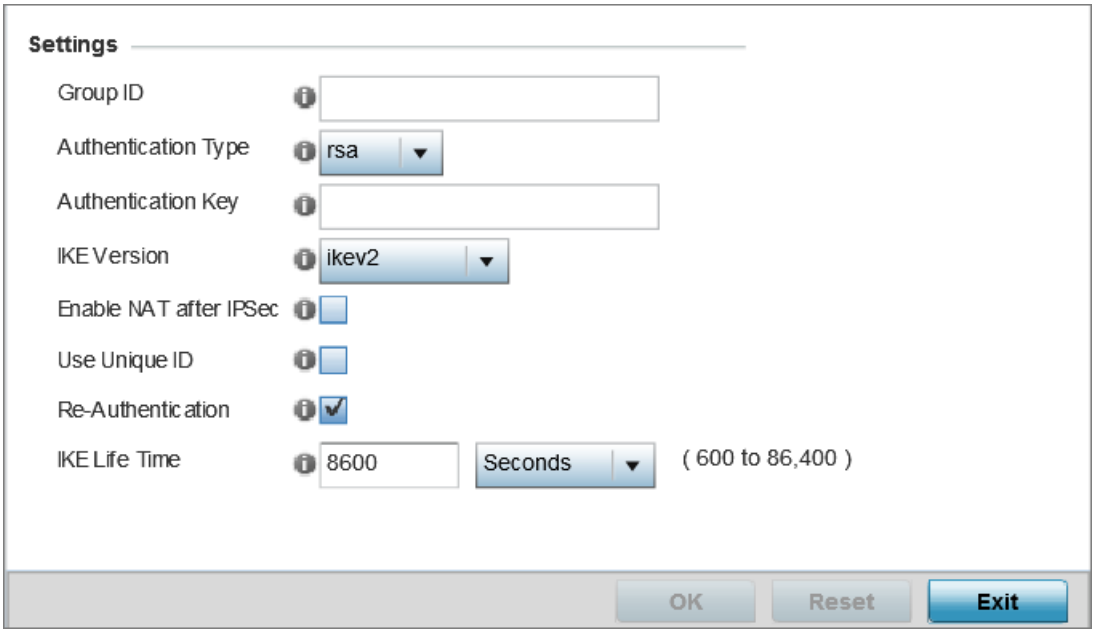



**Figure 222: Profile Overrides - Security - Auto IPSec Tunnel Configuration Screen**

4 Refer to the following table to configure the Auto IPSec Tunnel settings:

| | |
|---|---|
| Group ID | Configure the ID string used for IKE authentication. String length can be between 1 and 64 characters. |
| Authentication Type | Set the IPSec Authentication Type. Options include **PSK** (Pre Shared Key) or **RSA**. |
| Authentication Key | Set the common key for authentication between the remote tunnel peer. Key length is between 8 and 21 characters. |
| IKE Version | Configure the IKE version to use. The available options are: **ikev1-main**, **ikev1- aggr** and **ikev2**. |
| Enable NAT after IPSec | Select this option to enable NAT after IPSec. Enable this if there are NATted networks behind VPN tunnels. |
| Use Unique ID | In scenarios having different access points behind different NAT boxes and routers have the same IP address, it is not possible to create a tunnel between the wireless controller and the access point because the wireless controller does not identify the access point uniquely. When this option is selected, each access point behind a same NAT box or router will have an unique ID which is used to create the VPN tunnel. |

| | |
|---|---|
| Re-Authentication | Select this option to re-authenticate the key on a IKE rekey. This setting is disabled by default. |
| IKE Life Time | Set a lifetime in either seconds (600 - 86,400), minutes (10 - 1,440), hours (1 - 24), or days (1) for IKE security association duration. The default setting is 8600 seconds. |

5 Click **OK** to save the Auto IPSec Tunnel configuration changes.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Settings

To override a profile's security settings:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Security** and select **Settings**.

The security settings configuration screen displays.

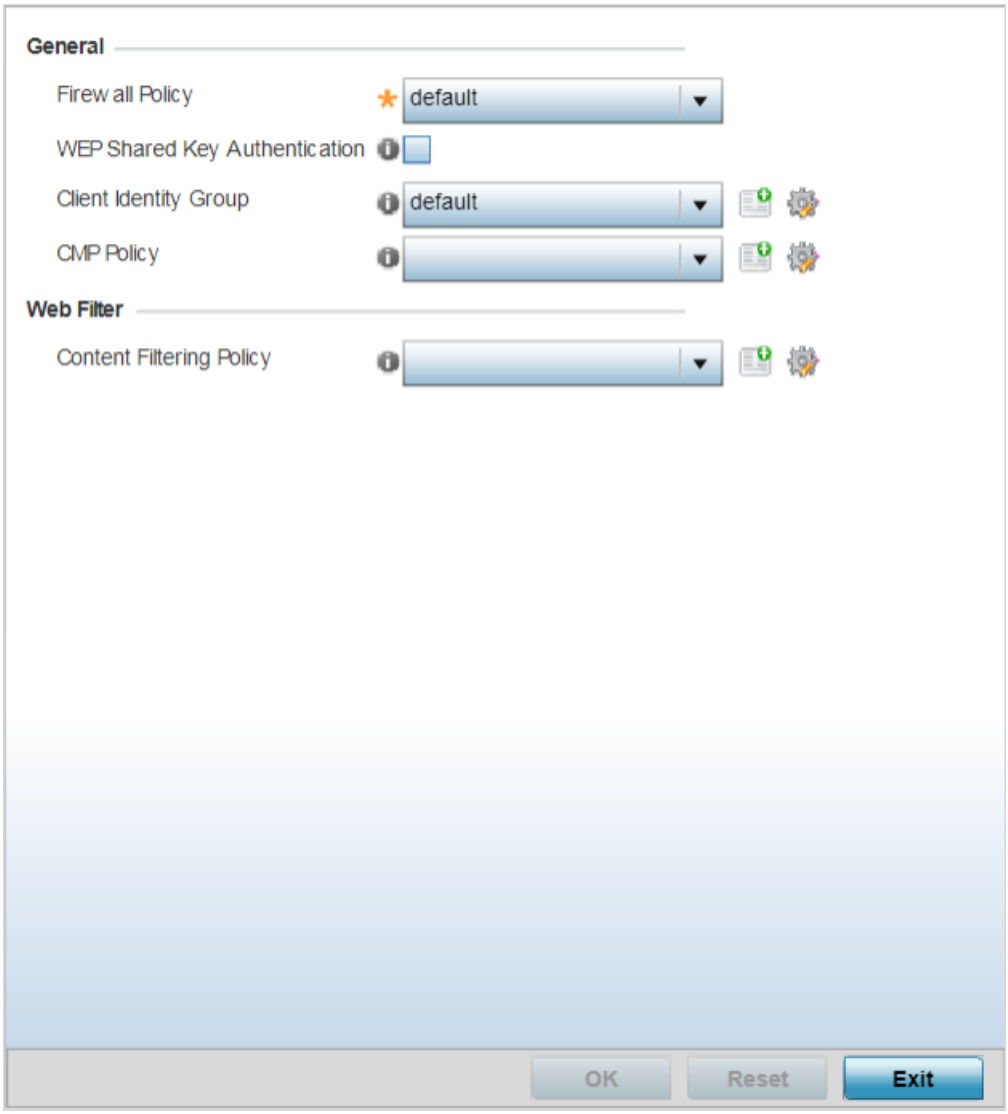



**Figure 223: Security Settings Configuration Screen**

4 Use the firewall policy from the Firewall Policy drop-down menu to select and apply a firewall policy on the device. The policy applied here will override the profile's firewall settings. Is an existing firewall policy does not meet your requirements, select the **Create** icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and edited as needed using the **Edit** icon.

5 Select the **WEP Shared Key Authentication** option override the profiles WEP key configuration at the device level. WEP keys are used to access the network. The access point, other proprietary routers, and our clients use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without our adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

6 Use the Client Identity Group drop-down menu to select the client identity group to use with this device. This setting overrides access point's profile client identity settings. A client identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for devices classes in the network. A client identity group is a collection of client identities that identify devices and applies specific permissions and restrictions on these devices. For more information, see Device Fingerprinting on page 762.

7 In the Web Filter field, use the Content Filtering Policy drop-down menu to select or override the URL Filter configuration on the access point.

Web filtering is used to restrict access to resources on the Internet. For more information on configuring Web Filtering policies, see Web Filtering on page 728.

### Profile Overrides - Certificate Revocation

A CRL *(certificate revocation list)* is a list of revoked certificates that are no longer valid. A certificate can be revoked if the CA *(certificate authority)* has improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is that the user is no longer in sole possession of the private key.

To override an access point profile's CRL configurations:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Security** and select **Certificate Revocation**.

The certificate revocation list (CRL) configuration screen displays.

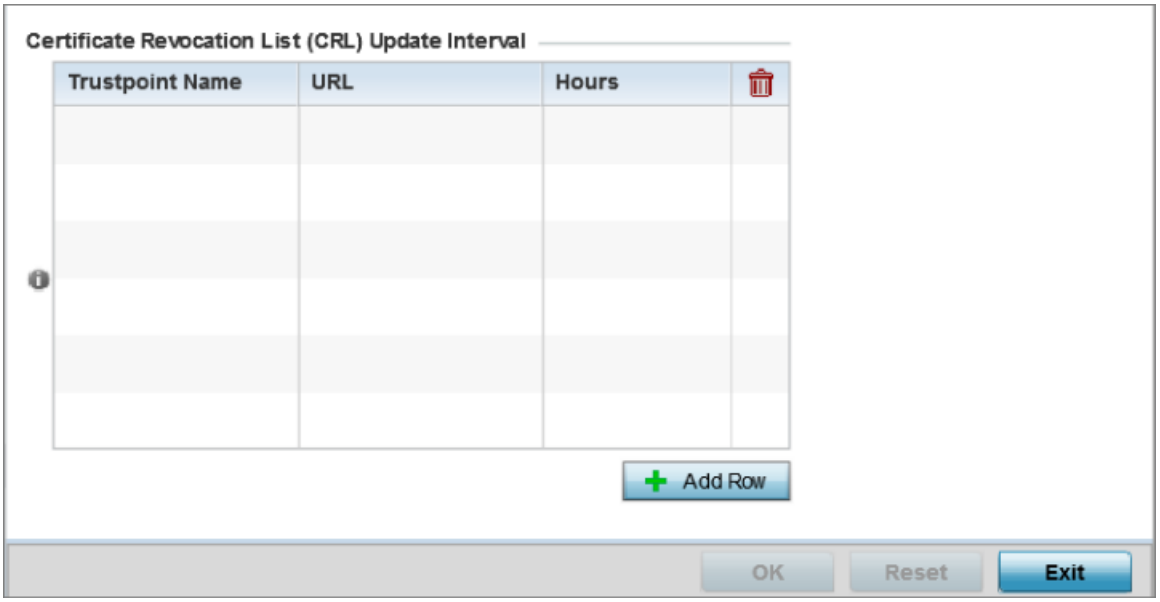



**Figure 224: Certificate Revocation List (CRL) Configuration Screen**

Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

4 In the Certificate Revocation List (CRL) Update Interval table, click **+ Add Row** and configure the following:

Use this option to quarantine certificates from use in the network. Additionally, a certificate can be placed on hold for a user defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.

| | |
|---|---|
| Trustpoint Name | Provide the name of the trustpoint. The name should not exceed 32 characters. |
| URL | Enter the third-party resource ensuring the trustpoint's legitimacy. |
| Hours | Use this spinner control to specify an interval (in hours) after which a device copies a CRL file from an external server and associates it with a trustpoint. |

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

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Trustpoints

A RADIUS certificate links identity information with a public key enclosed in the certificate. A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.

To override a RADIUS Trustpoint configuration at the device level:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides → Security** and select **Trustpoints**.

The trustpoints configuration screen displays.

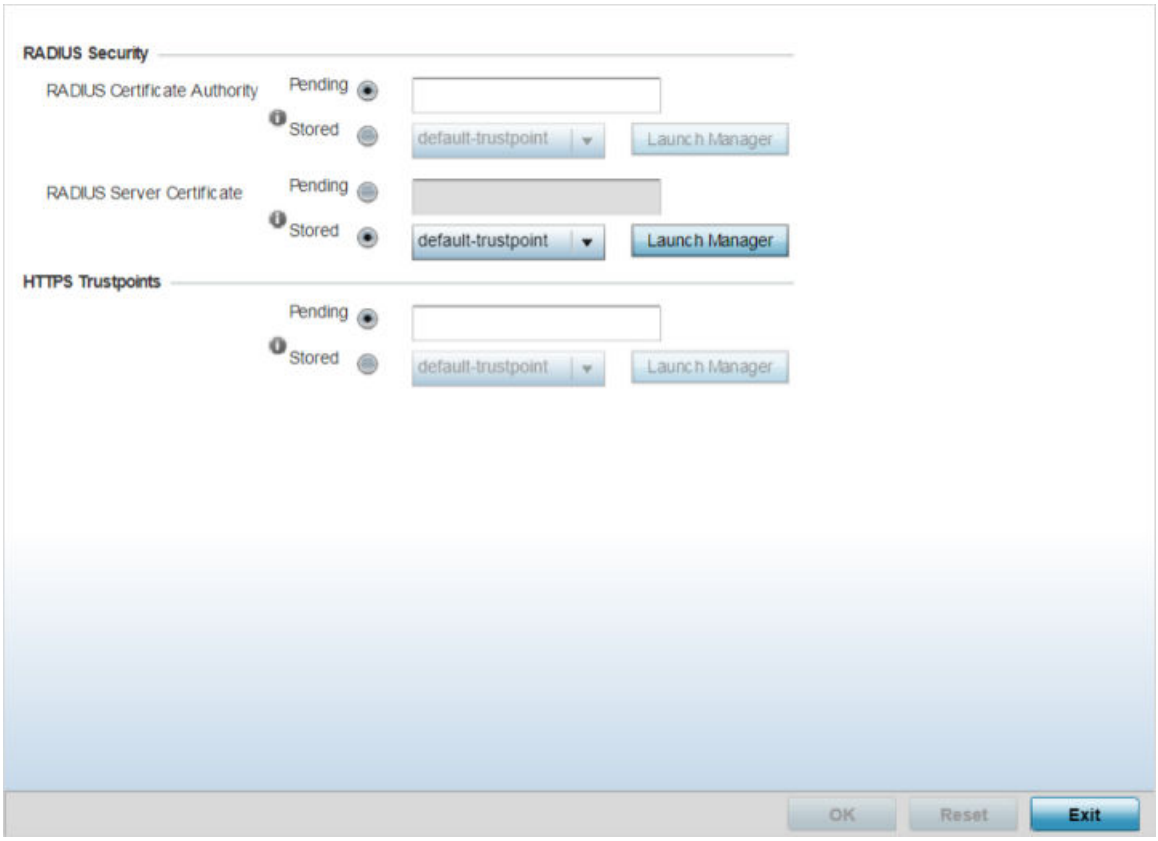



**Figure 225: Trustpoints Configuration Screen**

4 Set the following **RADIUS Security** certificate settings:

| | |
|---|---|
| RADIUS Certificate Authority | Select **Pending** to use a certificate that is in the process of being created or is yet to be created. As such certificates will not be listed under the Stored drop-down, use this method instead. Using this option is not a guarantee that the trust point will work as intended if the trust point is not loaded on to the device. The trust point can be created later, however, it must be present on the device when the device is deployed.<br>Select **Stored** to enable a drop-down menu where an existing certificate can be leveraged or use default-trustpoint. To leverage an existing certificate, click the **Launch Manager** button. |
| RADIUS Server Certificate | Select **Pending** radio button to use a certificate that is in the process of being created or is yet to be created. As such certificates will not be listed under the Stored drop-down, use this method instead. Using this option is not a guarantee that the trust point will work as intended if the trust point is not loaded on to the device. The trust point can be created later, however, it must be present on the device when the device is deployed.<br>Select **Stored** to enable a drop-down menu where an existing certificate can be leveraged or use default-trustpoint. To leverage an existing certificate, click the **Launch Manager** button. |

5 In the HTTPS Trustpoints field, set the following parameters:

| | |
|---|---|
| HTTPS Trustpoint | Select **Pending** to use a certificate that is in the process of being created or is yet to be created.<br>Select **Stored** to enable a drop-down menu where an existing certificate/trustpoint can be used. where an existing certificate can be leveraged or use default-trustpoint. To leverage an existing certificate, click the **Launch Manager** button. For more information, see Certificate Management on page 891. |

6 Click **OK** to save the RADIUS Trustpoints configuration overrides.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - NAT Pool

NAT *(Network Address Translation)* is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller, service platform or access point managed network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

Additionally, NAT is a process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping one IP address to another. In most deployments NAT is used in conjunction with IP masquerading which hides RFC1918 private IP addresses behind a single public IP address.

NAT can provide a profile outbound internet access to wired and wireless hosts connected to a controller, service platform or access point. Many-to-one NAT is the most common NAT technique for outbound internet access. Many-to-one NAT allows a controller, service platform or access point to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

Note

The wiNG 7.1 release does not support NAT on AP505 and AP510 model access points. This feature will be supported in future releases.

To override an access point profile's NAT configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides → Security** and select **NAT**.

The NAT Pool screen displays by default. This screen lists the NAT policies that have been created thus far. Any of these policies can be selected and applied to a profile.

Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

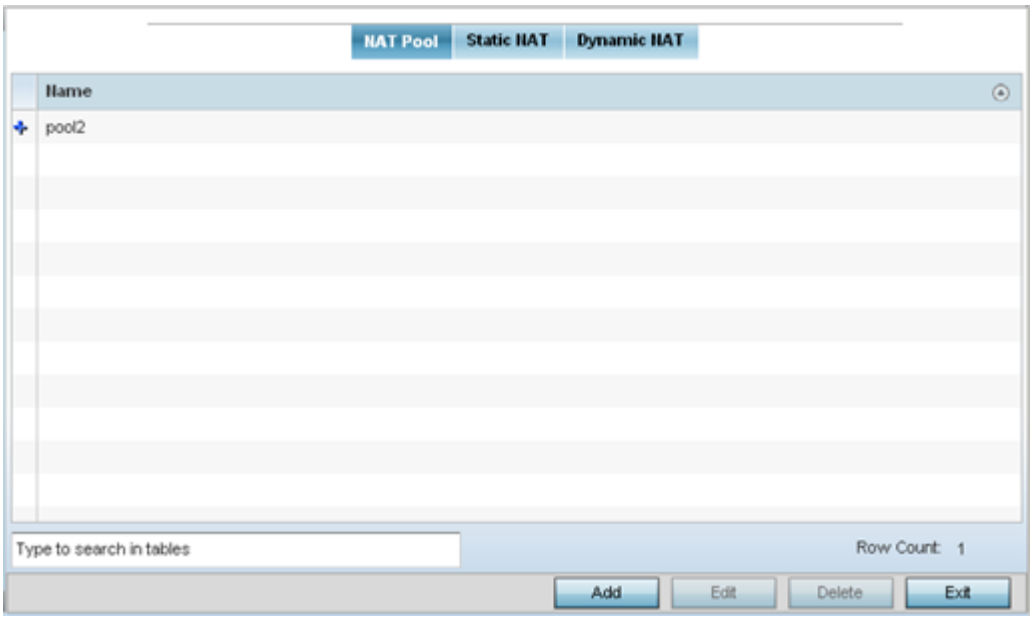



**Figure 226: Profile Overrides - Security - NAT Pool Main Screen**

4 To modify an existing NAT policy, select it and click **Edit**.

To create a new NAT policy, click **Add**. To delete an obsolete NAT policy, select it and click **Delete**.

The NAT Pool window displays.

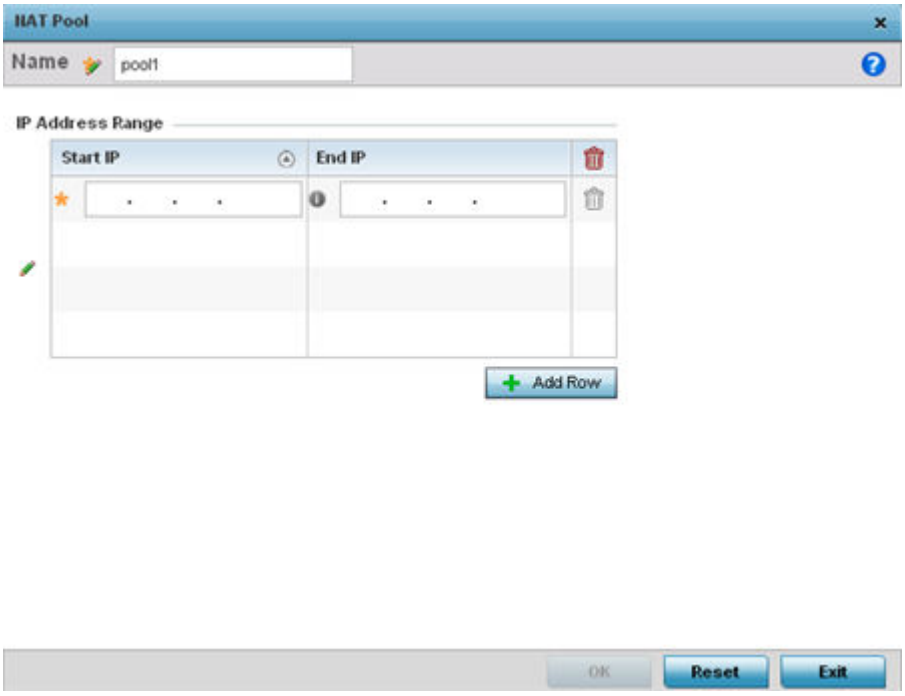



**Figure 227: NAT Configuration - Add/Edit NAT Pool Window**

5 If adding a new NAT policy, in the Name field, provide a `name` to help distinguish it from others with similar configurations.

6 In the IP Address Range table, click **+ Add Row** and define a range of IP addresses.

The IP addresses defined here are hidden from the public internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from potentially being routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

| | |
|---|---|
| Start IP | Enter the first IP address in the range |
| End IP | Enter the last IP address in the range. |

7 Click **OK** to save the NAT pool configuration changes.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Static NAT - Source

*Static NAT* creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a web server on a perimeter interface with the internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

To override the static NAT source and destination configurations:

1 Select the **Static NAT** tab.

The Source screen displays by default and lists existing static NAT configurations. Existing static NAT configurations are not editable, but new configurations can be added or existing ones deleted as they become obsolete.

The **Static NAT → Source** screen displays by default.

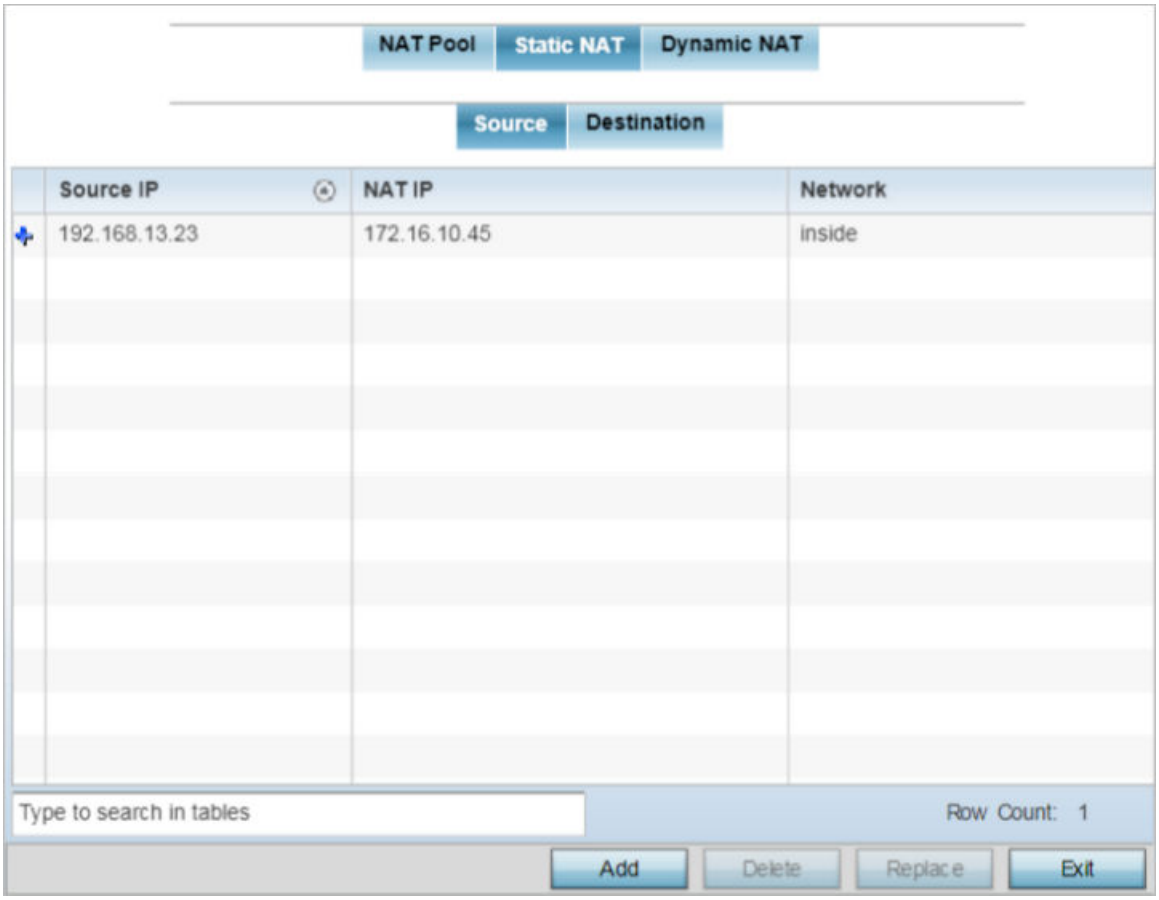



**Figure 228: NAT Configuration - Static NAT - Source Main Screen**

2 To remove an existing source IP address, from an internal network, to NAT IP address mapping, select the configuration and click **Delete**.

Existing NAT source configurations cannot be edited.

3 To create a new source IP address, from an internal network, to a NAT IP address click **Add**.

The Add Source NAT window displays.

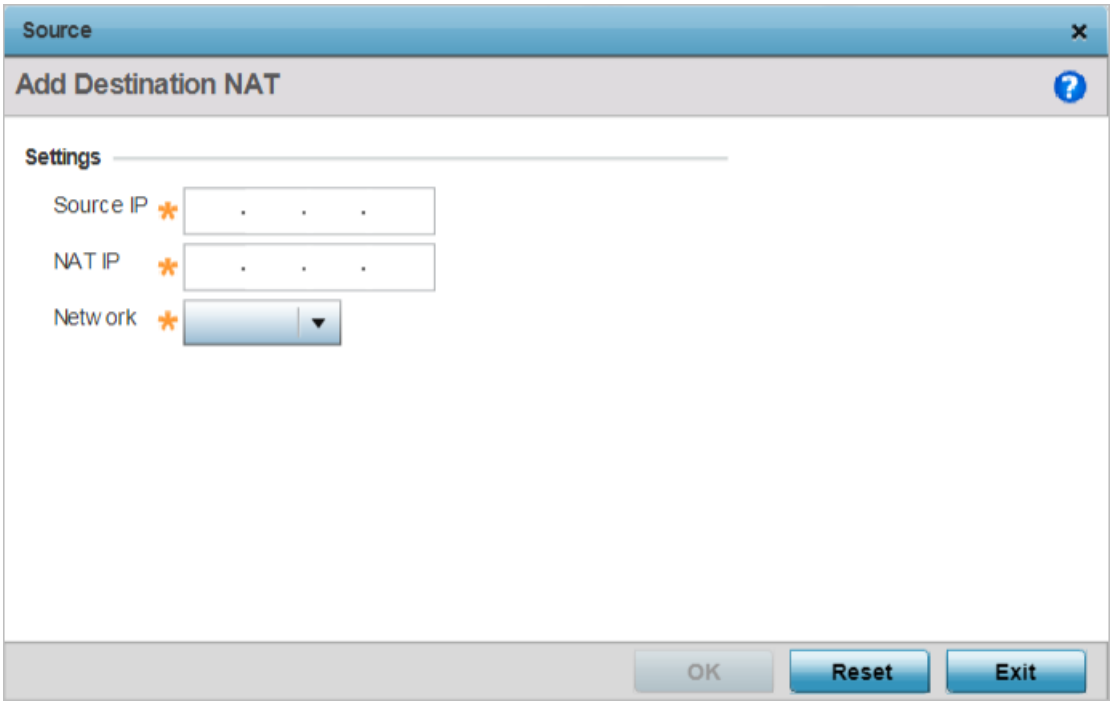



**Figure 229: NAT Configuration - Add Static NAT Source IP Address Window**

4 Define the following parameters:

| | |
|---|---|
| Source IP | Enter the address used at the (internal) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination. |
| NAT IP | Enter the IP address of the matching packet to the specified value. The IP address modified can be either **source** or **destination** based on the direction specified. |
| Network | Select **Inside** or **Outside** NAT as the network direction. The default setting is Inside.<br>Select *Inside* to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a web server on a perimeter interface with the internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host. |

5 Click **OK** to save the static NAT source configuration changes.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Static NAT - Destination

NAT destination configurations define the way in which packets passing through the NAT on the way back to the LAN are searched against the records kept by the NAT engine. The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the network.

1 Select the **Destination** tab.

The **Static NAT** → **Destination** screen displays.

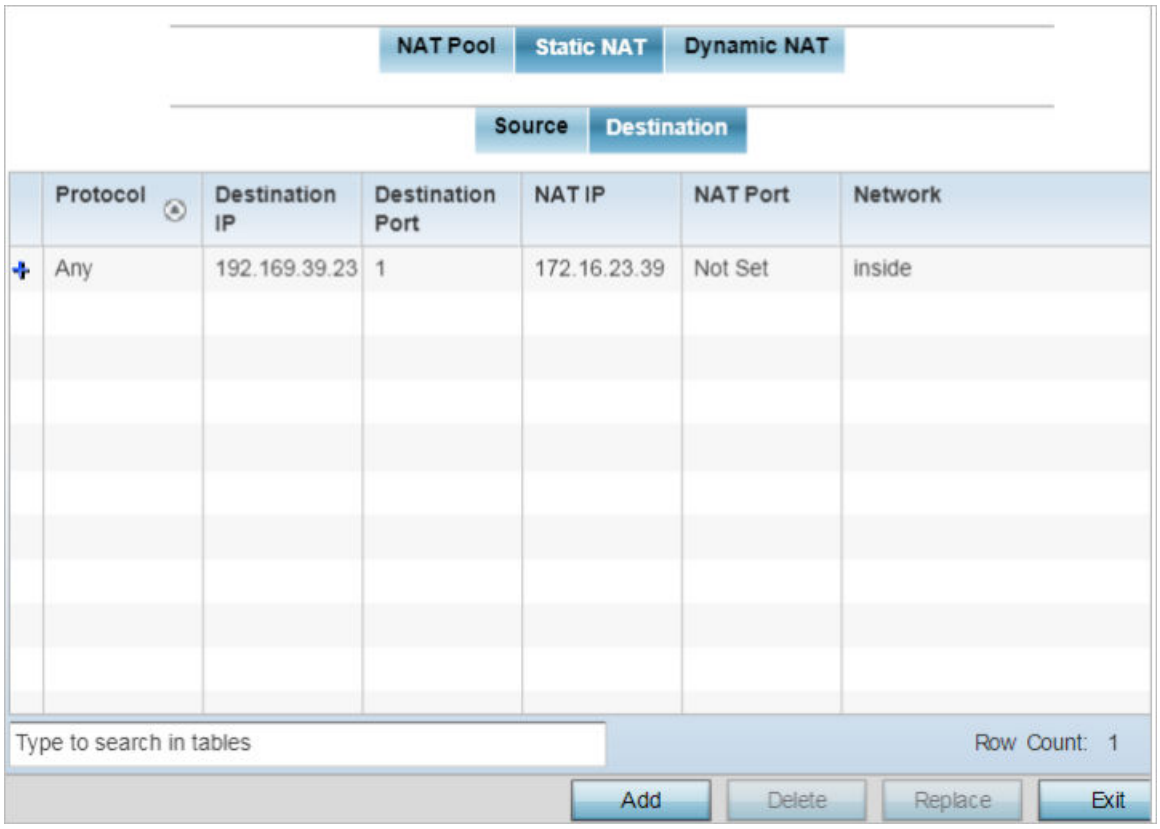



**Figure 230: NAT Configuration - Static NAT - Destination Main Screen**

2 Review existing Static NAT destination configurations to determine if a new configuration warrants creation or an existing configuration warrants modification or deletion.

3 To permanently remove a NAT destination, select it and click **Delete**.

Existing NAT destination configurations cannot be edited.

4 To create a new NAT destination configuration, click **Add**.

The Add Destination NAT window displays.

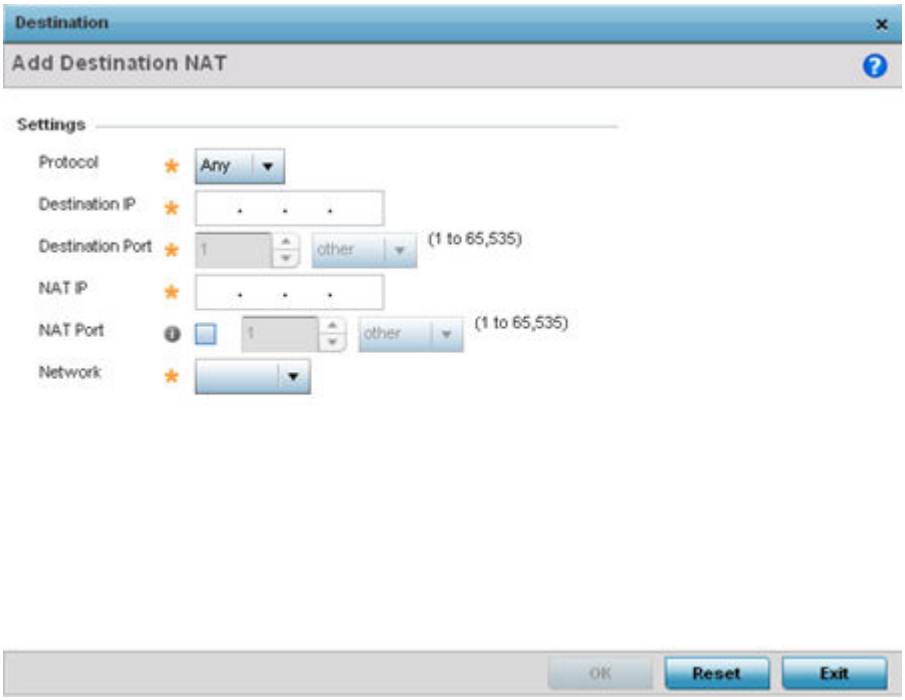



**Figure 231: NAT Configuration - Add Static NAT Destination IP Address Window**

5 Set or override the following destination configuration parameters.

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a web server on a perimeter interface with the internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

| | |
|---|---|
| Protocol | Select the protocol for use with static translation. Available options are **TCP**, **UDP** and **Any**. The default setting is *Any*.<br>TCP is a transport layer protocol used by applications requiring guaranteed delivery. It is a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number.<br>The UDP *(User Datagram Protocol)* offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. |
| Destination IP | Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination. |

| | |
|---|---|
| Destination Port | Set the local port number used at the (source) end of the static NAT configuration. The default value is port 1. |
| NAT IP | Enter the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified. |
| NAT Port | Enter the port number of the matching packet to the specified value. This option is valid only if the direction specified is **destination**. |
| Network | Select **Inside** or **Outside** NAT as the network direction. The default setting is Inside.<br>Select Inside to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a web server on a perimeter interface with the internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host. |

6 Click **OK** to save the static NAT destination configuration changes.

Click **Reset** to revert to the last saved configuration.

Profile Overrides - Dynamic NAT

Dynamic NAT configurations translate the IP address of packets going out from one interface to another interface based on configured conditions. Dynamic NAT requires packets be switched through a NAT router to generate translations in the translation table.

To override the dynamic NAT configurations:

1 Select the **Dynamic NAT** tab.

The Dynamic NAT main screen displays by default.

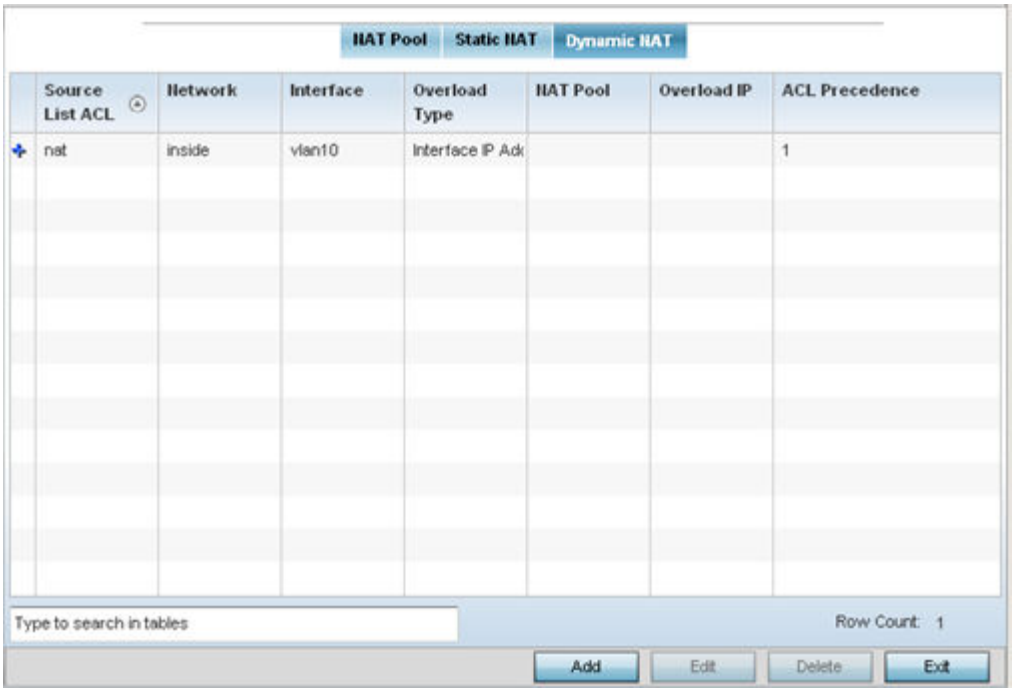



**Figure 232: NAT Configuration - Dynamic NAT Main Screen**

2 Review the following to determine whether a new dynamic NAT configuration needs to be created, or whether an existing one can be edited or deleted:

| | |
|---|---|
| Source List ACL | Lists an ACL to define the packet selection criteria for the NAT configuration. NAT is applied only on packets which match a rule defined in the access-list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination. |
| Network | Displays **`Inside`** or **`Outside`** NAT as the network direction for the dynamic NAT configuration. |
| ACL Precedence | Lists the administrator-assigned priority set for the listed source list ACL. The lower the value listed, the higher the priority assigned to this ACL rule. |
| Interface | Lists the VLAN (from 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. |
| Overload Type | Displays the overload type used when several internal addresses are NATed to only one or a few external addresses. Options include **`NAT Pool`**, **`One Global Address`** and **`Interface IP Address`**. The default setting is Interface IP Address. |
| NAT Pool | Displays the name of an existing NAT pool used with the dynamic NAT configuration. |
| Overload IP | If **`One Global IP Address`** is selected as the **Overload Type**, define an IP address to use as a filter address for the IP ACL rule. |

3 To modify an existing dynamic NAT configuration, select it and click **Edit**. To remove an existing configuration, select it and click **Delete**.

4 To create a new dynamic NAT configuration, click **Add**.

The Source window displays.

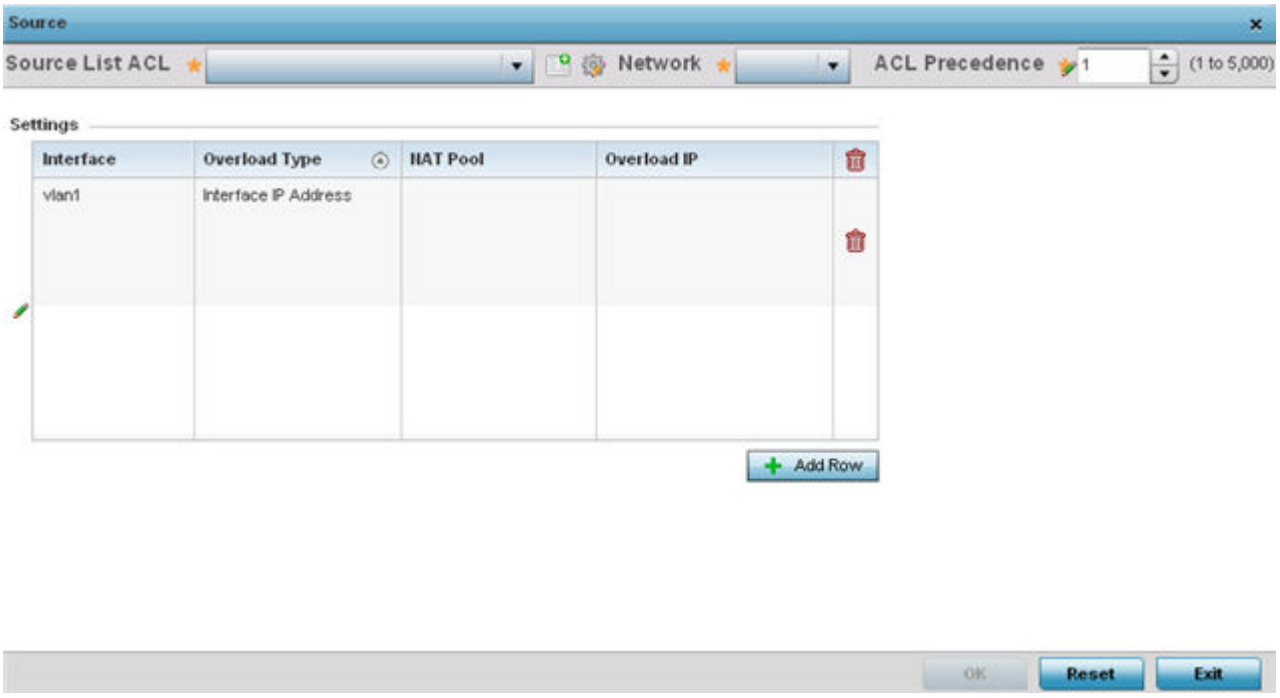



**Figure 233: Profile Overrides - Security - NAT - Dynamic NAT - Source ACL List Screen**

5 Set or override the following to define the Dynamic NAT configuration:

| | |
|---|---|
| Source List ACL | Select an ACL name to define the packet selection criteria for NAT. NAT is applied only on packets which match a rule defined in the access-list. These addresses (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination. |
| Network | Select **Inside** or **Outside** NAT as the network direction for the dynamic NAT configuration. **Inside** is the default setting. |
| ACL Precedence | Set the priority (from 1 - 5000) for the source list ACL. The lower the value, the higher the priority assigned to the ACL rule. |
| Interface | Select the VLAN (from 1 - 4094) or WWAN used as the communication medium between the source and destination points within the NAT configuration. Ensure that the VLAN selected adequately supports the intended network traffic within the NAT supported configuration. |
| Overload Type | Define the overload type used when several internal addresses are NATed to only one or a few external addresses. Options include **NAT Pool**, **One Global Address**, and **Interface IP Address**. The default setting is Interface IP Address. |

| | |
|---|---|
| NAT Pool | Provide the name of an existing NAT pool for use with the dynamic NAT configuration.<br><br>Note:<br>This option is enabled only if the Overload Type is set or **`NAT Pool`**. |
| Overload IP | If **`One Global IP Address`** is selected as the **Overload Type**, define an IP address to use as a filter address for the IP ACL rule. |

6 Click **OK** to save the dynamic NAT configuration changes.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Bridge NAT

Use Bridge NAT to manage Internet traffic originating at a remote site. In addition to traditional NAT functionality, Bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router.

Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

Note

Bridge NAT supports single AP deployments only. This feature cannot be used in a branch deployment with multiple access points.

To override an access point profile's Bridge NAT configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Security** and select **Bridge NAT**.

The Bridge NAT configuration screen displays.

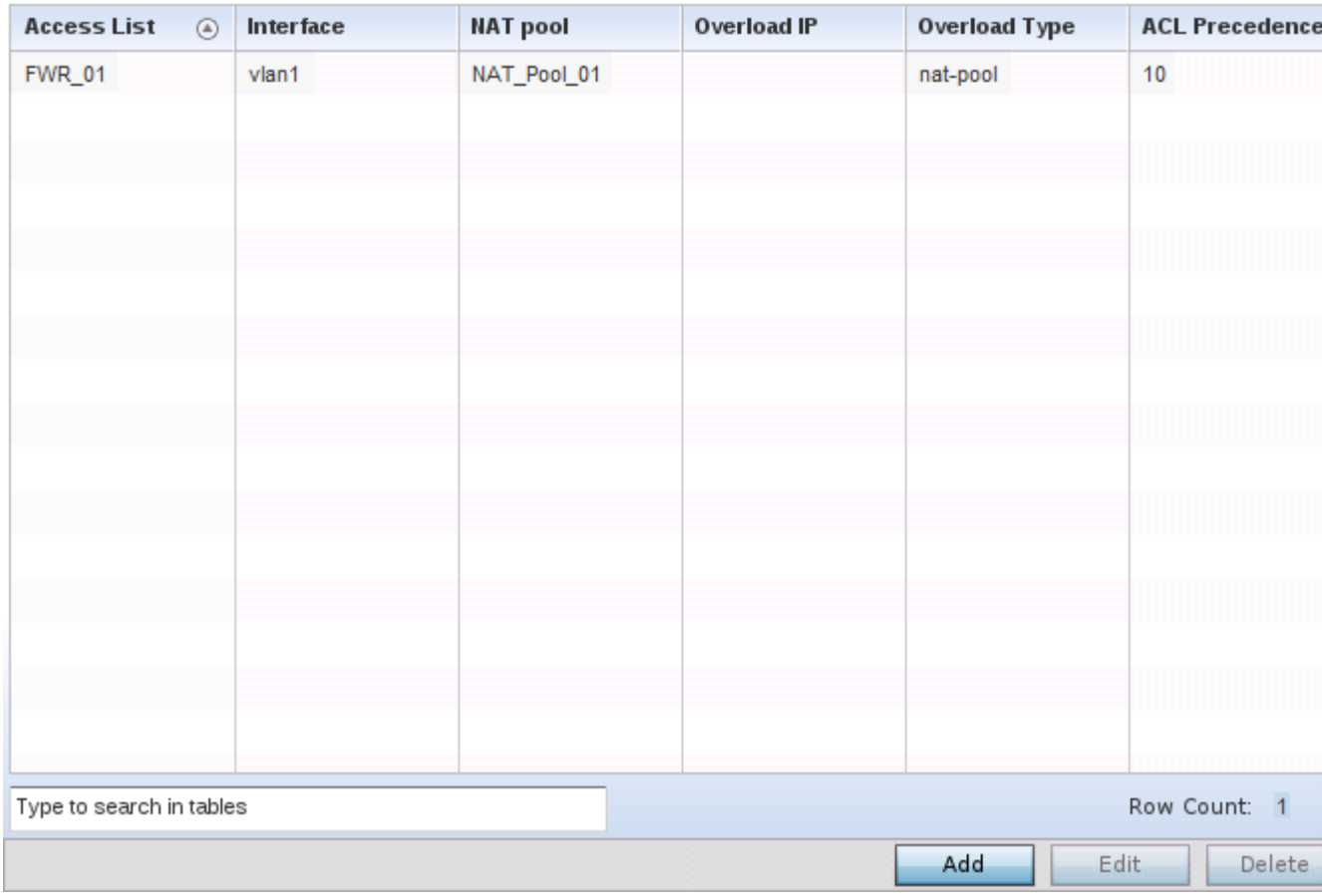



**Figure 234: Profile Overrides - Bridge NAT Configuration - Main Screen**

4 Review the following to determine whether a new Bridge NAT configuration requires creation or an existing configuration modified or removed:

| | |
|---|---|
| Access List | Lists the ACL applying IP address **access**/**deny** permission rules to the Bridge NAT configuration. |
| Interface | Lists the communication medium (outgoing layer 3 interface) between source and destination points. This is either the access point's **pppoe1** or **wwan1** interface or the VLAN used as the redirection interface between the source and destination. |
| NAT Pool | Lists the names of existing NAT pools used with the Bridge NAT configuration. This displays only when the Overload Type , in the Bridge NAT configuration, is set to **NAT Pool**. |
| Overload IP | Lists the IP address used globally for numerous local addresses. |
| Overload Type | Lists the overload type used with the listed IP ACL rule. Displays as either **NAT Pool**, **One Global Address** or **Interface IP Address**. |
| ACL Precedence | Lists the administrator assigned priority set for the ACL. The lower the value, higher is the priority assigned to the ACL rules. |

5 To override an existing Bridge NAT configuration, select it from the displayed list and click **Edit**.

To create a new Bridge NAT configuration, click **Add**. To delete an obsolete configuration, select it and click **Delete**.

The Dynamic NAT configuration window displays.

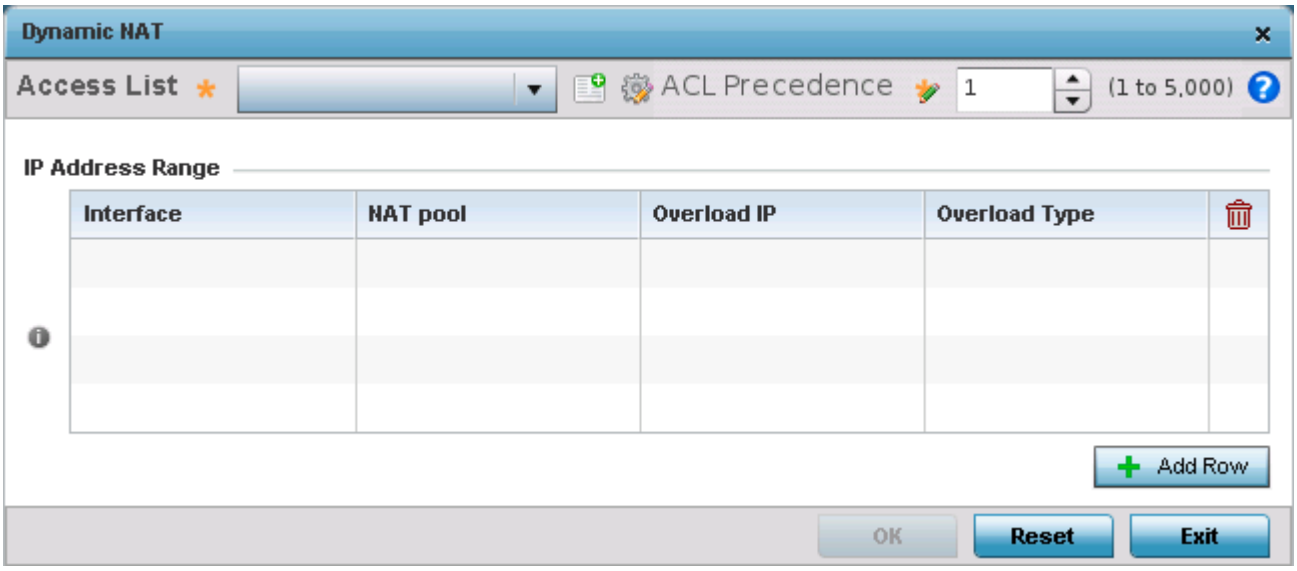



**Figure 235: Profile Overrides - Bridge NAT - Add/Edit Dynamic NAT Window**

6 Use the Access List drop-down menu to select and apply an ACL to the policy based forwarding rule.

A new ACL can be defined by selecting the **Create** icon, or an existing set of IP ACL rules can be modified by selecting the **Edit** icon.

7 In the IP Address Range table, review the existing IP addresses and address ranges configured to access the Internet.

| | |
|---|---|
| Interface | Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an access point WWAN or PPPoE interface. Traffic can also be redirected to a designated VLAN. |
| NAT Pool | Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to NAT Pool. |
| Overload IP | Lists the IP address used to represent a large number local addresses for this configuration. |
| Overload Type | Displays the override type for this policy based forwarding rule. |

8 Select **+ Add Row** to set new IP Address Range settings for the Bridge NAT configuration.

The Add Row window displays.

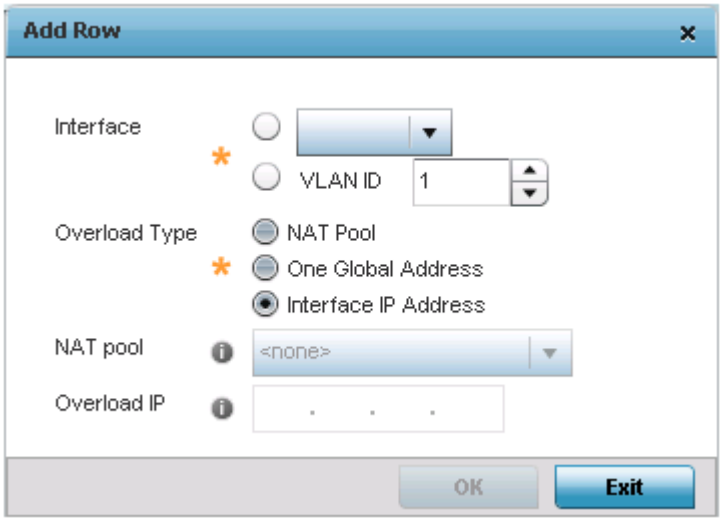



**Figure 236: Bridge NAT - Dynamic NAT - Add IP address and Address Configuration Window**

9 Select **OK** to save the Add Row and Dynamic NAT screens.

Select **Reset** to revert to the last saved configuration.

### Profile Overrides - Application Visibility (AVC)

DPI *(Deep packet inspection)* is an advanced packet filtering technique functioning at the application layer. Use DPI to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the WiNG managed network. The contents of each packet are scanned, occasionally logged and blocked or routed to their destination. Deep packet inspection helps an ISP block the spread of viruses, illegal downloads and prioritize data transmitted by bandwidth-heavy applications (video and VoIP applications) to help prevent network congestion.

Note

Application Visibility is available only on AP 7562, AP-8432 and AP-8533 access points.

To override an access point profile's AVC configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Security** and select **Application Visibility (AVC)**.

Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

The Application Visibility (AVC) configuration screen displays.

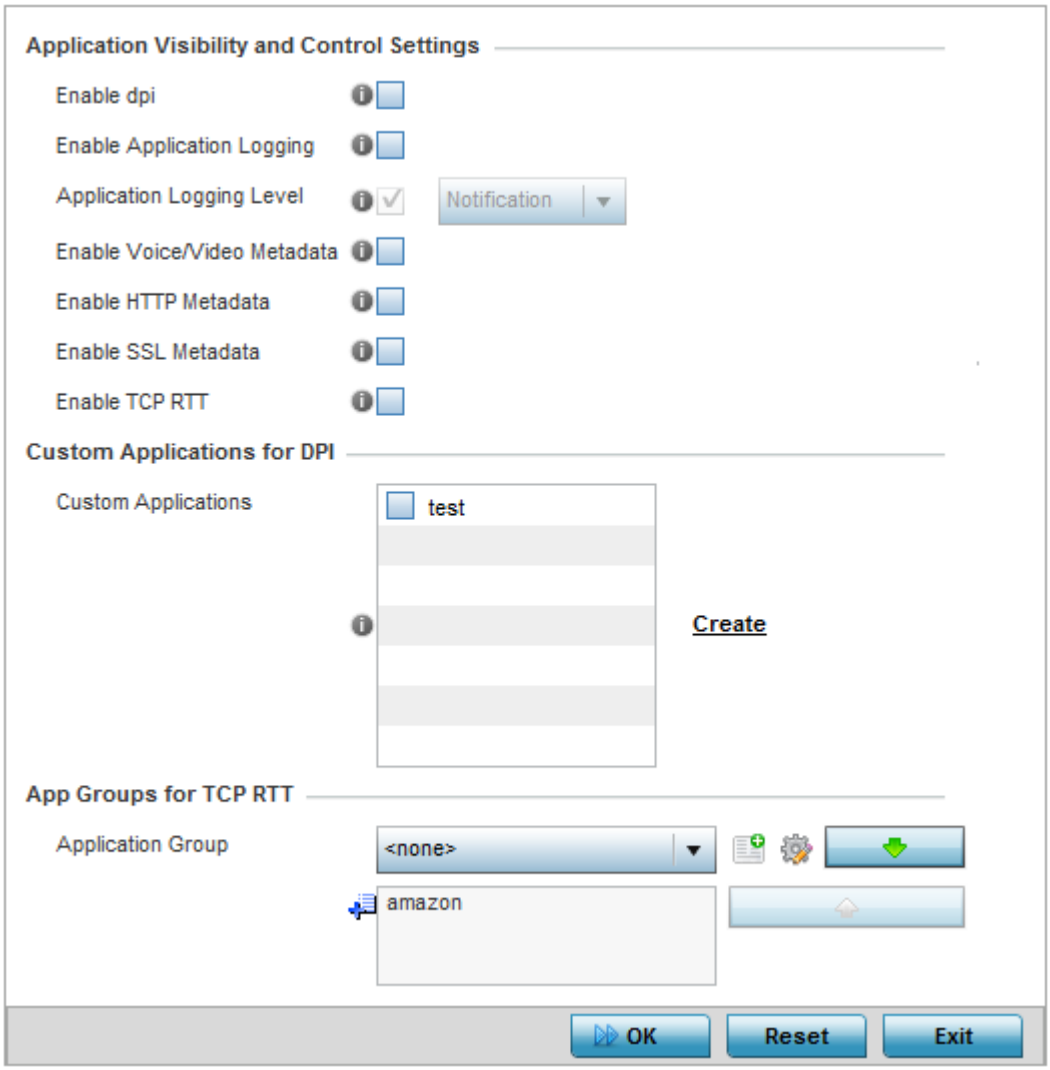



**Figure 237: Profile Overrides - Application Visibility (AVC) Configuration Screen**

4 Set or override the following Application Visibility and Control Settings:

| | |
|---|---|
| Enable dpi | Enable this setting to provide deep-packet inspection (application assurance) by inspecting every byte of each application header packet passing through the controller or service platform. When enabled, application data streams are inspected at a granular level to help prevent viruses and spyware from accessing the WiNG managed network. |
| Enable Applications Logging | Select this option to enable event logging for DPI application recognition. This setting is disabled by default. |
| Applications Logging Level | If enabling DPI application recognition event logging, set the logging level. Severity levels include **`Emergency`**, **`Alert`**, **`Critical`**, **`Errors`**, **`Warning`**, **`Notice`**, **`Info`**, and **`Debug`**. The default logging level is *Notification*. |
| Enable Voice/Video Metadata | Select this option to enable the metadata extraction from voice and video classified flows. The default setting is disabled. |
| Enable HTTP Metadata | Select this option to enable extraction of metadata from HTTP application data flows. The default setting is disabled. |
| Enable SSL Metadata | Select this option to enable extraction of metadata from SSL application data flows. The default setting is disabled. |
| Enable TCP RTT | Select this option to enable extraction of RTT information from TCP flows. The default setting is disabled. |

5 Review the Custom Applications for DPI field to select the custom applications available for this device profile.

For information on creating custom applications and their categories, see Application on page 718.

6 If you are enabling TCP-RTT metadata collection, use the App Groups for TCP RTT field to specify the application groups for which TCP-RTT metadata collection is to be enabled.

Select the **Application Groups** from the drop-down menu and use the green, down arrow to move the selection to the box below. You can add a maximum of eight groups to the list.

If the desired application group is not available, select the **Create** icon to define a new application group configuration or select the **Edit** icon to modify an existing application group. For information on creating custom application groups, see Application on page 718.

7 Click **OK** to save the changes or overrides.

Click **Reset** to revert to the last saved configuration.

### *Profile Overrides - VRRP*

A default gateway is a critical resource for connectivity. However, it's prone to a single point of failure. Thus, redundancy for the default gateway is required by the access point. If WAN backhaul is available, and a router failure occurs, then an access point should act as a router and forward traffic on to its WAN link.

Define an external VRRP *(Virtual Router Redundancy Protocol)* configuration when router redundancy is required in a wireless network requiring high availability.

The election of a VRRP master is central to the configuration of VRRP. A VRRP master (once elected) performs the following functions:

To override an access point profile's VRRP configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides**, and select **VRRP**.

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

The VRRP → VRRP configuration screen displays by default.

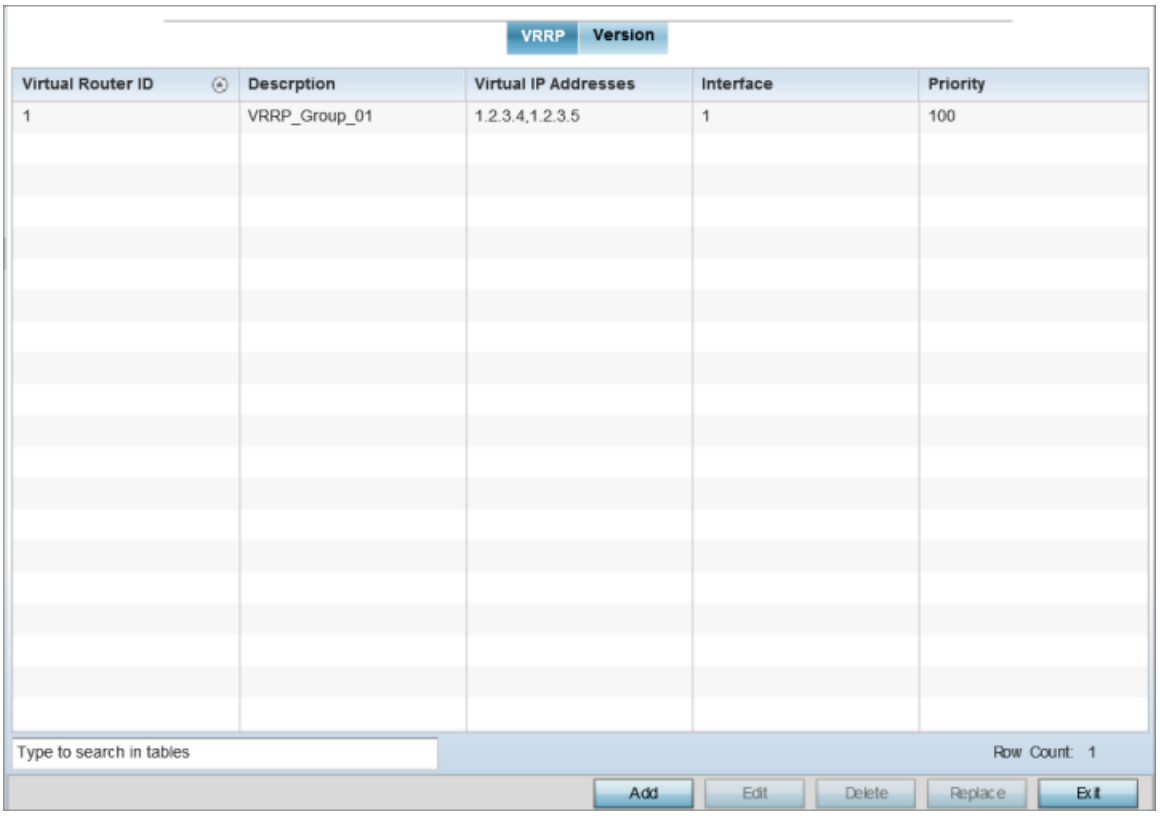



**Figure 238: Profile Overrides - VRRP - VRRP Configuration Main Screen**

4 Review the following VRRP configuration data to assess whether a new VRRP configuration is required or whether an existing VRRP configuration can be modified or removed:

| | |
|---|---|
| Virtual Router ID | A numerical index (from 1 - 255) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router for which a packet is reporting status. |
| Description | A description assigned to the VRRP configuration when it was either created or modified. The description is implemented to provide additional differentiation beyond the numerical virtual router ID. |
| Virtual IP Addresses | The virtual interface IP address used as the redundant gateway address for the virtual route. |

| | |
|---|---|
| Interface | The interfaces selected on the access point to supply VRRP redundancy failover support. |
| Priority | A numerical value (from 1 - 254) used for the virtual router master election process. The higher the numerical value, the higher the priority in the election process. |

5 Click **Add** to create a new VRRP configuration.

Click **Edit** to modify or override the attributes of a existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by clicking **Delete**.

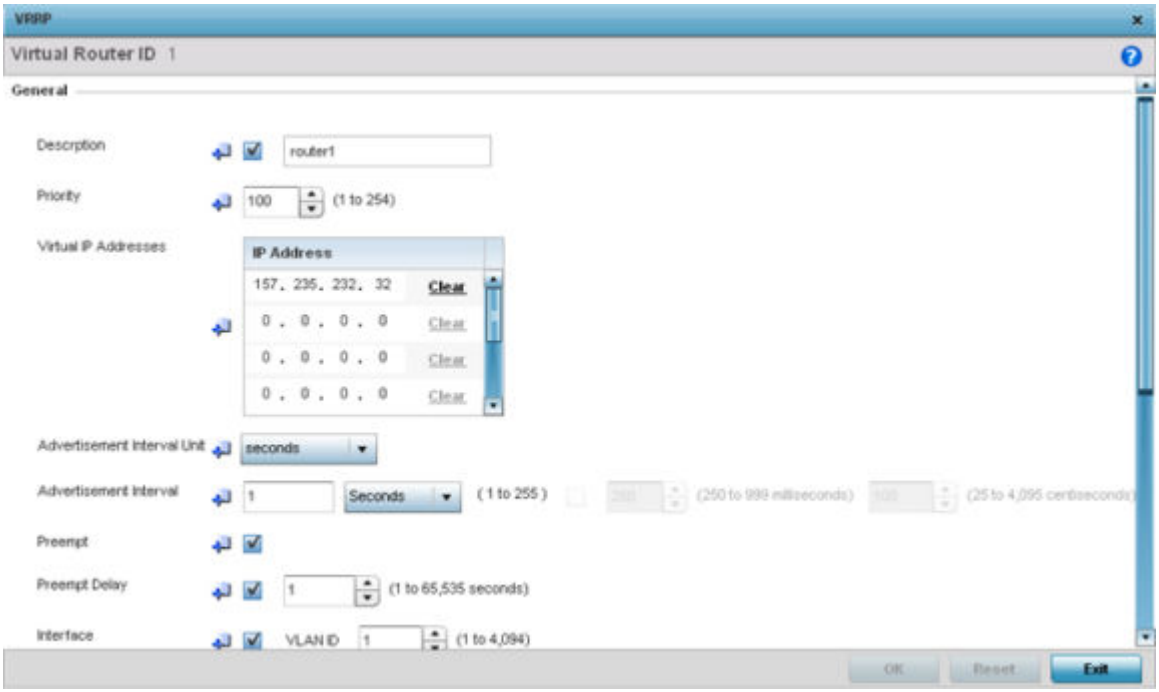



**Figure 239: Device Overrides - VRRP - Virtual Router Screen**

6 If you are creating a new VRRP configuration, assign a **Virtual Router ID** from 1 - 255.

In addition to functioning as numerical identifier, the ID identifies the virtual router for which a packet is reporting status.

7 Define the following VRRP General parameters:

| | |
|---|---|
| Description | In addition to an ID assignment, a virtual router configuration can be assigned a textual description (up to 64 characters) to further distinguish it from others with a similar configuration. |
| Priority | Use the spinner control to set a VRRP priority setting from 1 - 254. The controller or service platform uses the defined setting as criteria in selection of a virtual router master. The higher the value, the greater the likelihood of this virtual router ID being selected as the master. |
| Virtual IP Addresses | Provide up to eight IP addresses representing the Ethernet switches, routers, or security appliances defined as virtual router resources. |

| | |
|---|---|
| Advertisement Interval Unit | Select either **seconds**, **milliseconds** or **centiseconds** as the unit used to define VRRP advertisements. After an option is selected, the spinner control becomes enabled for that Advertisement Interval option. The default interval unit is seconds.<br>If you are changing the VRRP group version from 2 to 3, the advertisement interval must be in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds. |
| Advertisement Interval | After an Advertisement Interval Unit is selected, use the spinner control to set the interval the VRRP master sends out advertisements on each of its configured VLANs. The default setting is 1 second. |
| Preempt | Select this option to ensure a high priority backup router is available to preempt a lower priority backup router resource. The default setting is enabled. When selected, the **Preempt Delay** option becomes enabled to set the actual delay interval for pre-emption. This setting determines if a node with a higher priority can take over all the Virtual IPs from the nodes with a lower priority. |
| Preempt Delay | If the **Preempt** option is selected, use the spinner control to set the delay interval (in seconds) for preemption. |
| Interface | Select this value to enable or disable VRRP operation and define the VLAN (1 - 4,094) interface where VRRP will be running. These are the interfaces monitored to detect a link failure. |

8 Refer to the Protocol Extension field to define the following:

| | |
|---|---|
| Sync Group | Select the option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP fail over if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled by default. |
| Network Monitoring: Local Interface | Select wwan1, pppoe1, and VLAN ID(s) as needed to extend VRRP monitoring to these local access point interfaces. Once selected, these interfaces can be assigned an increasing or decreasing level or priority for virtual routing in the VRRP group. |
| Network Monitoring: Critical Resource | Assign the priority level for the selected local interfaces. Backup virtual routers can increase or decrease their priority in case the critical resources connected to the master router fail, and then transition to the master state themselves. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include **None**, **increment-priority** and **decrement priority**. |
| Network Monitoring: Delta Priority | Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring is enabled, the value is incremented by the setting defined. |

9 Click **OK** to save the VRRP configuration changes.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - VRRP Version

To set or override the VRRP Version configuration:

1 Select the **Version** tab to define the VRRP version scheme used with the configuration.

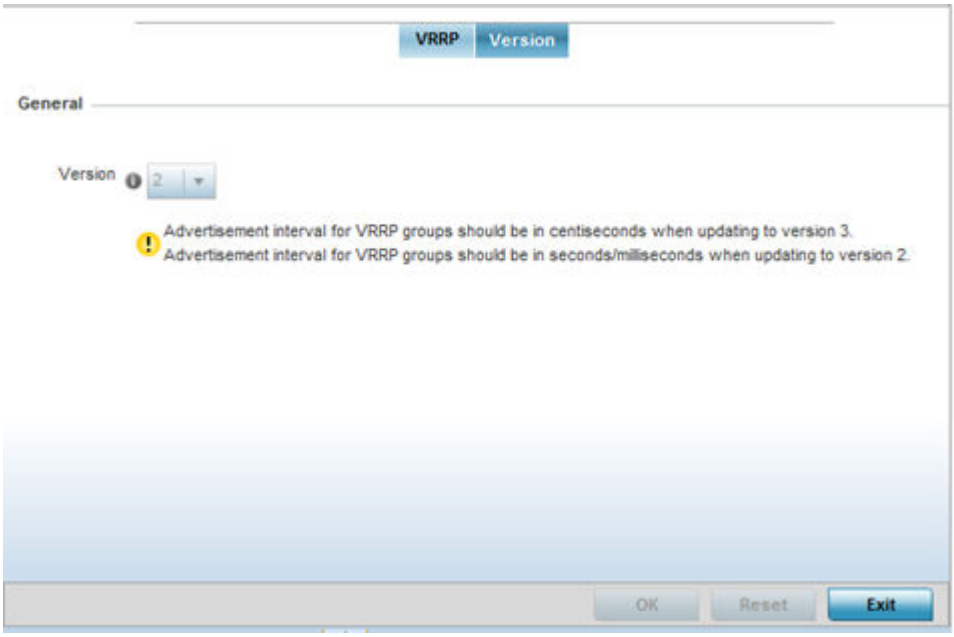



**Figure 240: Device Overrides - VRRP Screen - Version Tab**

VRRP version 3 (RFC 5798) and 2 (RFC 3768) are selectable to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. For more information on the VRRP protocol specifications (available publicly) refer to http://www.ietf.org/rfc/rfc3768.txt (version 2) and http://www.ietf.org/rfc/rfc5798.txt (version 3).

2 Click **OK** to save the VRRP Version configuration changes.
Click **Reset** to revert to the last saved configuration.

3

*Profile Overrides - List of Critical Resources*

Critical resources are device IP addresses or interface destinations on the network inter-operated as critical to the health of the network. The critical resource feature allows for the continuous monitoring of these addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, a AAA server, a WAN interface, or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly by the access point. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, no critical resource policy is enabled, and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they are discovered. For example, a critical resource on the same subnet as the access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to monitored on that VLAN.

Critical resources configured for access point profiles, can be overridden at the device level. To override an access point profile's critical resource configuration:

1 Go to **Configuration → Devices → Device Overrides**.
The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides**, and select **Critical Resources**.

The List of Critical Resources screen displays by default.

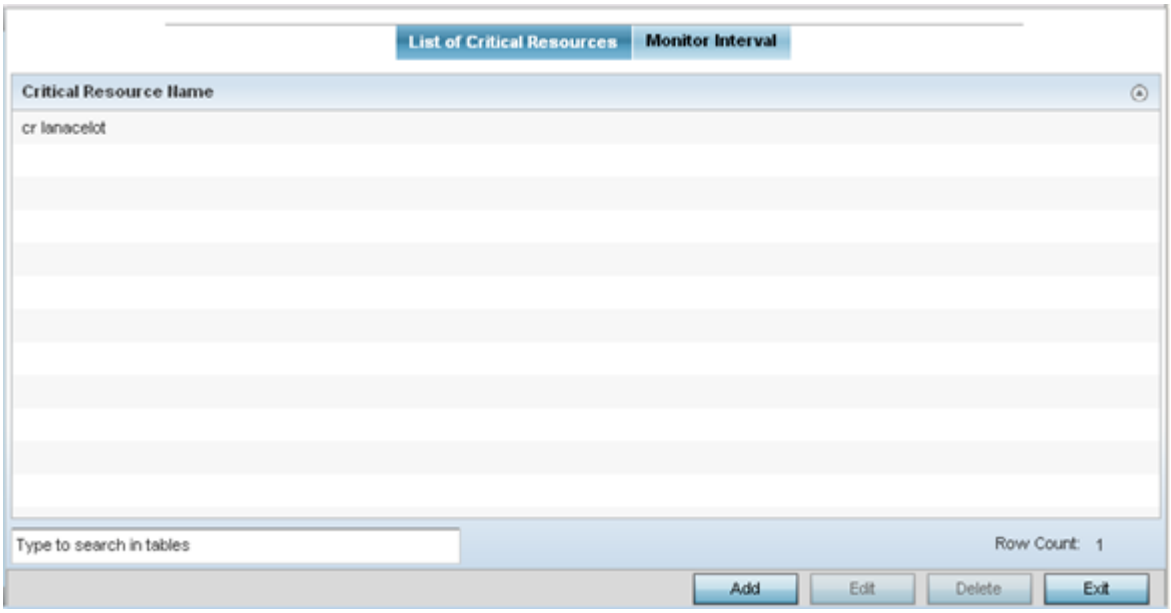



**Figure 241: Profile Overrides - Critical Resources - List of Critical Resources Screen**

The screen lists the destination IP addresses or interfaces (VLAN, WWAN, or PPPoE) used for critical resource connection. IP addresses can be monitored directly by the access point or controller. However, a VLAN, WWAN, or PPPoE must be monitored behind an interface.

4 To set or override an existing critical resource configuration, click **Edit**.

Click **Add** to add a new critical resource and connection method.

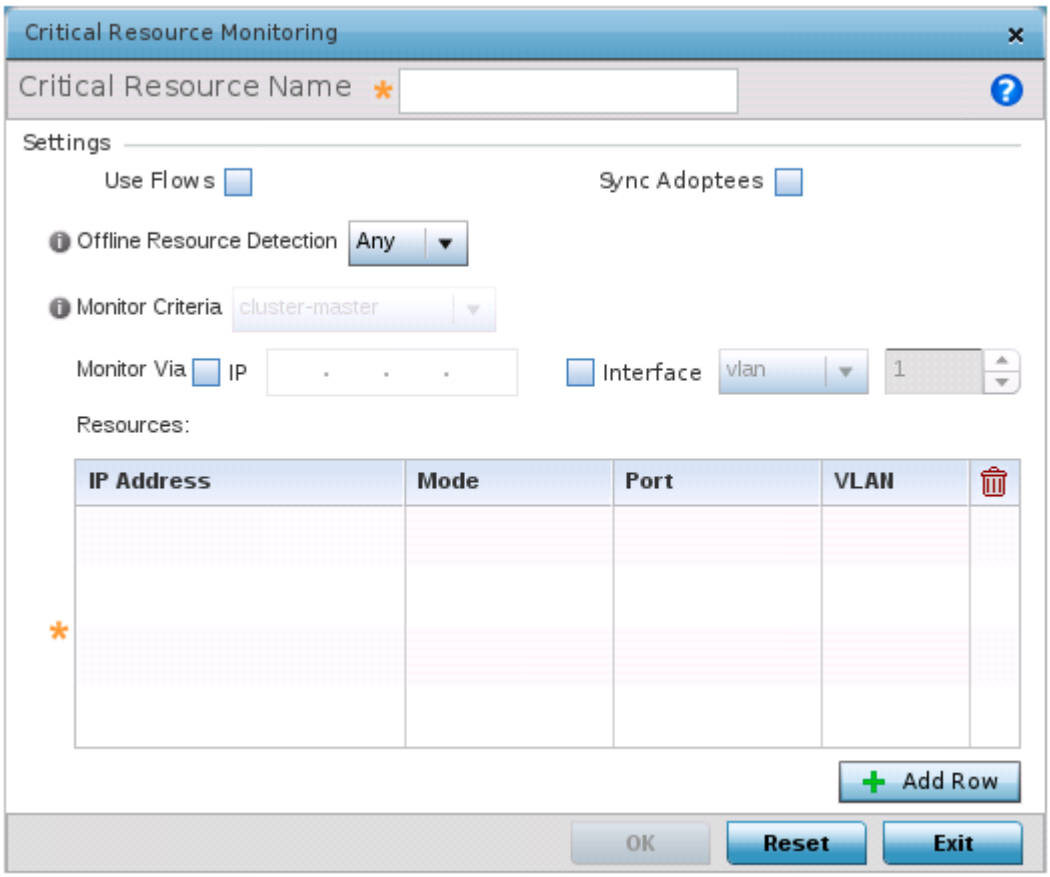



**Figure 242: Critical Resources Screen - Adding a Critical Resource**

5 If you are adding a new critical resource, in the Critical Resource Name field, provide a `name` up to 32 characters.

6 Select **Use Flows** so that the critical resource will monitor using firewall flows for DHCP or DNS instead of ICMP or ARP packets.

This reduces the amount of traffic on the network. This setting is disabled by default.

7 Select **Sync Adoptees** to sync adopted devices to state changes with a resource-state change message .

This setting is disabled by default.

8 Use the **Offline Resource Detection** drop-down menu to define how critical resource event messages are generated.

Options include **`Any`** and **`All`**. If you select **`Any`**, an event is generated when the state of any single critical resource changes. If you select **`All`**, an event is generated when the state of all monitored critical resources change.

9 Use the **Monitor Criteria** drop-down menu to select either **`rf-domain-manager`**, **`cluster-master`** or **`All`** as the resource for monitoring critical resources by one device and updating the rest of the devices in a group.

If you select rf-domain-manager, the current rf-domain manager performs resource monitoring, and the rest of the devices do not. The RF-domain-manager updates any state changes to the rest of the devices in the RF Domain.

With the cluster-master option, the cluster master performs resource monitoring and updates the cluster members with state changes.

With a controller-managed RF Domain, set **Monitoring Criteria** to **`All`** because the controller might not know the VLAN bridged locally by the devices in the RF Domain monitoring DHCP.

10 In the Monitor Via field, select the **`IP`** option to monitor a critical resource directly (within the same subnet) using the provided IP address as a network identifier.

11 In the Monitor Via field, select the **Interface** check box to monitor a critical resource using the critical resource's **`VLAN`**, **`WWAN1`** or **`PPPoE1`** interface.

If you select **`VLAN`**, use the spinner control to define the destination VLAN ID used as the interface for the critical resource.

12 In the Resources table, click **+ Add Row** and define the following parameters:

| | |
|---|---|
| IP Address | Provide the IP address of the critical resource. This is the address used by the access point to ensure the critical resource is available. Up to four addresses can be defined. |
| Mode | Set the ping mode used when the availability of a critical resource is validated. The options are:<br>• **`arp-only`** – Use only the ARP *(Address Resolution Protocol)* for pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known.<br>• **`arp-and-ping`** – Use both ARP and ICMP *(Internet Control Message Protocol)* for pinging the critical resource and sending control messages (for example, *device not reachable* or *requested service not available*). |
| Port | Provide the port on which the critical resource is available. Use the spinner control to set the port number. |
| VLAN | Using the spinner control, define the VLAN on which the critical resource is available. |

13 Click **OK** to save the critical resource configuration changes.

Click **Reset** to revert to the last saved configuration.

### Critical Resources - Monitor Interval

To override the critical resource monitoring interval configuration:

1 Select the **Monitor Interval** tab.

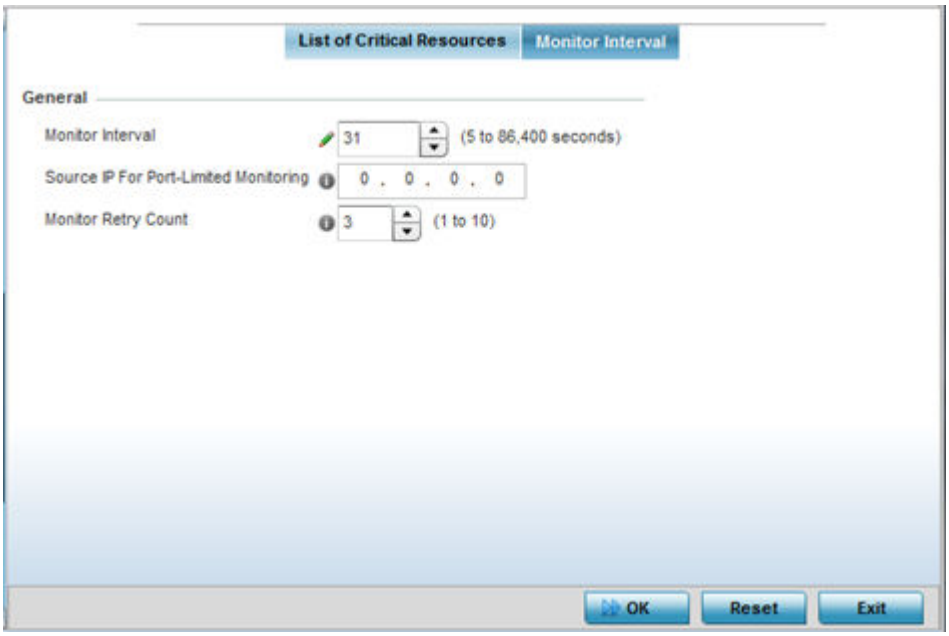



**Figure 243: Critical Resources Screen - Monitor Interval Tab**

2 Use **Monitor Interval** to set the duration, in seconds, between two successive pings to the critical resource.

Select a duration between 5 and 86,400 seconds. The default setting is 30 seconds.

3 Use **Source IP for Port-Limited Monitoring** to define the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface.

Generally, the source address 0.0.0.0 is used in the ARP packets used to detect critical resources. However, some devices do not support that IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for Port-Limited Monitoring must be different from the IP address configured on the device.

4 Use **Monitor Retry Count** to set the number of retry connection attempts (1 - 10) permitted before this device connection is defined as down (offline).

The default setting is three connection attempts.

5 Click **OK** to save the and monitor interval changes.

Click **Reset** to revert to the last saved configuration.

*Profile Overrides - Services*

Use this option to override the guest access (captive portal) server configurations. You can also override the RADIUS server, DHCP server, Bonjour Gateway Forwarding Policy, and Imagotag Policy service settings.

To set or override the access point profile's services configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** and select **Services**.

The Services configuration screen displays.

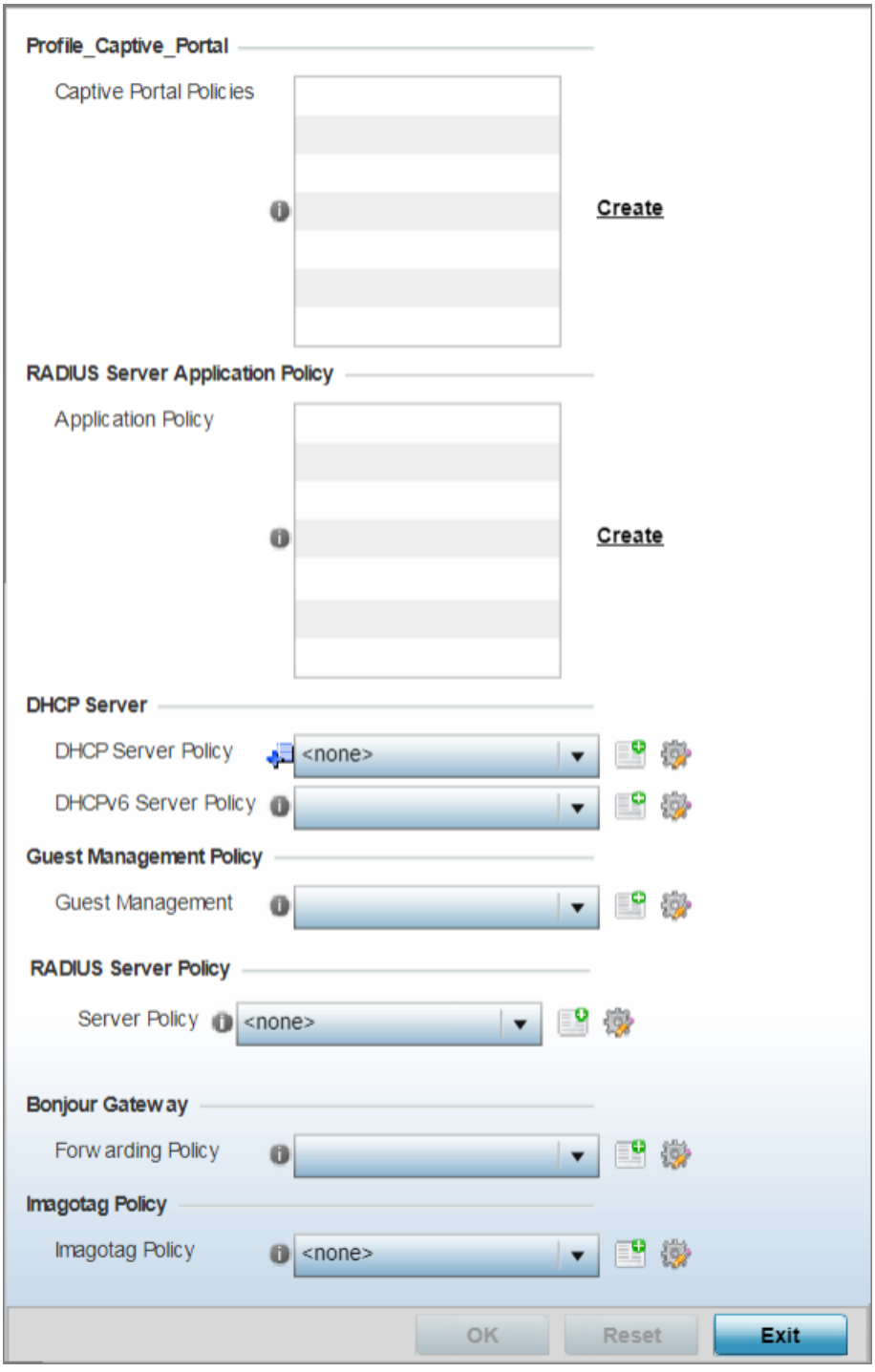



**Figure 244: Profile Overrides - Service Configuration Screen**

4 In the Captive Portal Policies box, select one of the existing captive portals displayed. If needed click the **Create** link to create a new captive portal configuration that can be applied to this profile.

A captive portal is guest access policy for providing guests temporary and restrictive access to the access point managed network.

A captive portal provides secure authenticated access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Agreement, Welcome and Fail pages provide the administrator with a number of options on screen flow and user appearance.

For more information, see Captive Portal Policies on page 785.

5 Use the **RADIUS Server Application Policy** drop-down menu to select an application policy to authenticate users and authorize access to the network.

A RADIUS policy provides the centralized management of authentication data (usernames and passwords). When an client attempts to associate, the controller or service platform sends the authentication request to the RADIUS server. If an existing RADIUS server policy does not meet your requirements, click the Create link to create a new policy.

6 Use the **DHCP Server Policy** drop-down menu assign this profile a DHCP server policy. If an existing DHCP policy does not meet the profile's requirements, click the Create icon to create a new policy configuration that can be applied to this profile, or click the Edit icon to modify the parameters of an existing DHCP Server policy.

DHCP *(Dynamic Host Configuration Protocol)* allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the onboard DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an predetermined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. When the lease expires, the client is no longer permitted to use the leased IP address. The profile's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired).

7 Use the **DHCPv6 Server Policy** drop-down menu assign this profile a DHCPv6 server policy. If an existing DHCP policy for IPv6 does not meet the profile's requirements, click the Create icon to create a new policy configuration that can be applied to this profile, or click the Edit icon to modify the parameters of an existing DHCP Server policy.

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network. DHCP in IPv6 works in with IPv6 router discovery. With the proper RA flags, DHCPv6 works like DHCP for IPv4. The central difference is the way a device identifies itself if assigning addresses manually instead of selecting addresses dynamically from a pool.

8 Use the **RADIUS Server Policy** drop-down menu to select an existing RADIUS server policy to use as a user validation security mechanism with this profile.

A profile can have its own unique RADIUS server policy to authenticate users and authorize access to the network. A profile's RADIUS policy provides the centralized management of controller or service platform authentication data (usernames and passwords). When an client attempts to associate, an authentication request is sent to the RADIUS server.

9 Refer to the **Bonjour Gateway** field to select or set a Bonjour Gateway Forwarding Policy.

Bonjour is Apple's implementation of Zeroconf *(zero-configuration)* networking. Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour Forwarding Policy enables discovery of services on VLANs which are not visible to the device running the Bonjour Gateway. Bonjour forwarding enables forwarding of Bonjour advertisements across VLANs to enable the Bonjour Gateway device to build a list of services and the VLANs where these services are available.

10 Refer to the **Imagotag Policy** field to select or set a Imagotag Policy. Use the drop-down menu to select and apply an Imagotag Policy to the AP's profile. You can use the **Create** to create a new policy or **Edit** icon to edit an existing policy. The Imagotag feature is supported only on the AP-8432 model access point.

For more information on enabling support for SES-imagotag's ESL tags on AP-8432 APs with USB interfaces, see Setting the Imagotag Policy on page 845.

11 Select **OK** to save services configuration overrides.

Select **Reset** to revert to the last saved configuration.

### *Profile Overrides - Management Settings*

There are mechanisms to allow or deny management access to the network for separate interfaces and protocols: HTTP, HTTPS, Telnet, SSH, and SNMP.

These management access configurations can be applied strategically to profiles as resource permissions dictate for the profile. Additionally, overrides can be applied to customize a device's management configuration, if deployment requirements change and a device's configuration must be modified from its original device profile configuration.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support. You can override the management configurations of a profile at the device level. To override an access point profile's management settings:

To define or override a profile's management configuration:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** → **Management**.

Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

The management Settings configuration screen displays.

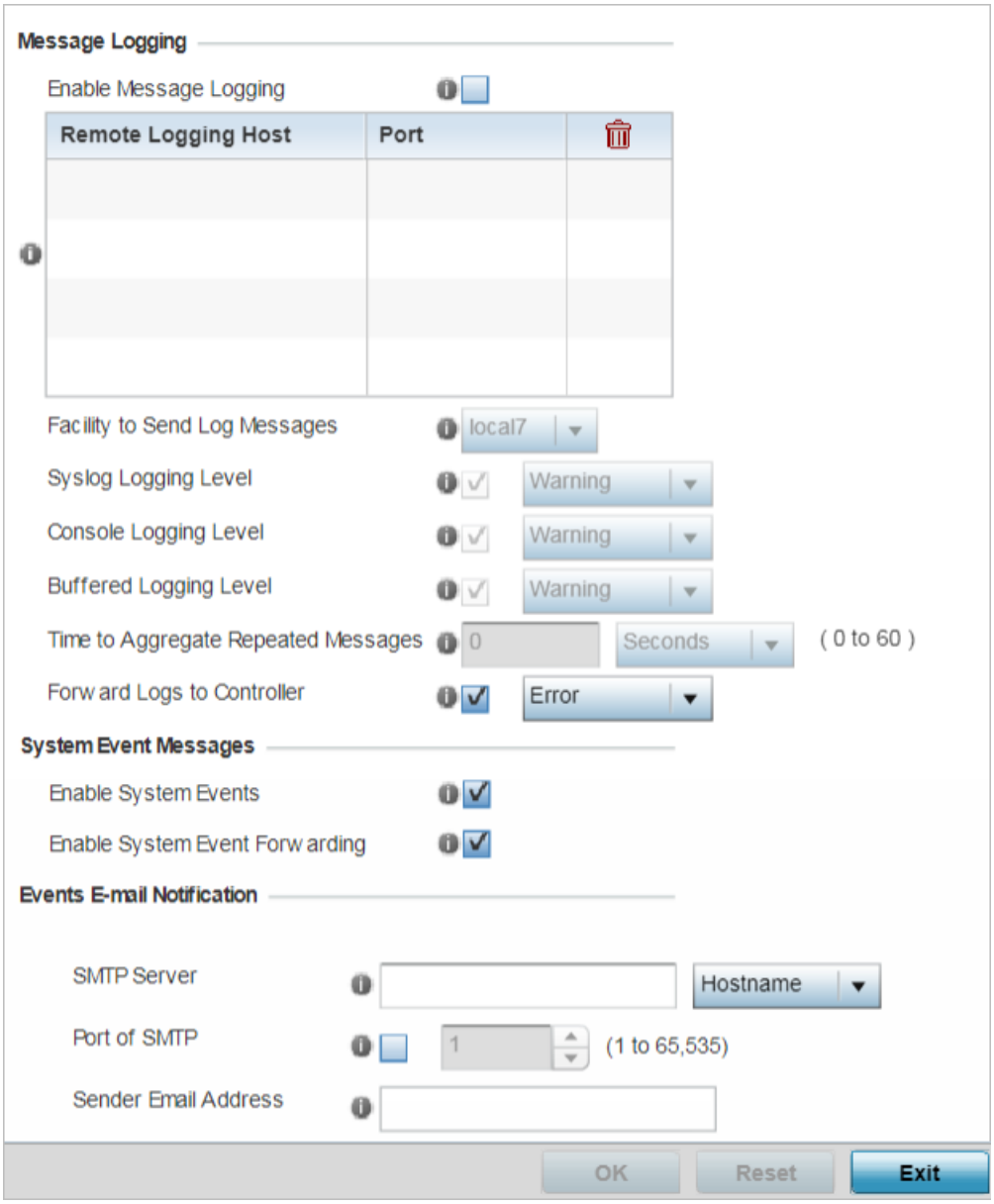



**Figure 245: Profile Overrides - Management - Settings Configuration Screen**

4 In the Message Logging field, select the **Enable Message Logging** checkbox to enable message logging. When enabled, system events are logged to a log file or a syslog server.

Selecting this check box enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.

5 In the Remote Logging Host table provide the following:

| | |
|---|---|
| Remote Logging Host | Define numerical (non DNS) IP addresses for up to four external resources where logged system events can be sent by the access point. Select the trash icon as needed to remove an IP address from the list. |
| Port | Define the ports at which the external resources are reachable. |

6 Configure the following Message Logging parameters:

| | |
|---|---|
| Facility to Send Log Messages | Use the drop-down menu to specify the local server (if used) for access point event log transfers. |
| System Logging Level | Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include: **0 - Emergency**, **1 - Alert**, **2 - Critical**, **3 - Errors**, **4 - Warning**, **5 - Notice**, **6 - Info** and **7 - Debug**. The default logging level is *4 - Warning*. |
| Console Logging Level | Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include: **0 - Emergency**, **1 - Alert**, **2 - Critical**, **3 - Errors**, **4 - Warning**, **5 - Notice**, **6 - Info** and **7 - Debug**. The default logging level is *4 - Warning*. |
| Buffered Logging Level | Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include: **0 - Emergency**, **1 - Alert**, **2 - Critical**, **3 - Errors**, **4 - Warning**, **5 - Notice**, **6 - Info** and **7 - Debug**. The default logging level is *4 - Warning*. |
| Time to Aggregate Repeated Messages | Define the increment (or interval) system events are logged on behalf of the access point. The shorter the interval, the sooner the event is logged. Either define an interval in seconds (0 - 60) or minutes (0 -1). The default value is 0 seconds. |
| Forward Logs to Controller | Select this option to define a log level for forwarding event logs to the control. Log levels include Emergency, Alert, Critical, Error, Warning, Notice, Info and Debug. The default logging level is Error. |

7 Refer to the System Event Messages field to define or override how system messages are logged and forwarded on behalf of the profile.

a Select **Enable System Events** to allow the profile to capture system events and append them to a log file.

It is important to log individual events to discern an overall pattern that may be negatively impacting performance. This setting is enabled by default.

b Select **Enable System Event Forwarding** to enable the forwarding of system events.

This setting is enabled by default.

8 Refer to the Events E-mail Notification field to define or override how system event notification emails are sent.

| | |
|---|---|
| SMTP Server | Specify either the hostname or IP address of the outgoing SMTP server where notification emails are originated. |
| Port of SMTP | If a non-standard SMTP port is used on the outgoing SMTP server, select this option and specify a port from 1 - 65,535 for the outgoing SMTP server to use. |
| Sender E-mail Address | Specify the email address from which notification email is originated. This is the *from* address on notification email. |

| | |
|---|---|
| Recipient's E-mail Address | Specify one or more email addresses to be the recipients of event email notifications. |
| Username for SMTP Server | Specify the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with an username and password before sending email through the server. |
| Password for SMTP Server | Specify password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with an username and password before sending email through the server. |

9 In the Persist Configuration Across Reloads field, use the **Configure** drop-down menu to define whether the access point saves a configuration received from a Virtual Controller AP to flash memory.

The configuration would then be made available if the this access point reboots and the Virtual Controller AP is not reachable. Options include **`Enabled`**, **`Disabled`**, and **`Secure`**.

10 Refer to the HTTP Analytics field to define analytic compression settings and update intervals.

| | |
|---|---|
| Compress | Select this option to use data compression to when sending updates to the controller. |
| Update Interval | Set the interval – in minutes, seconds, or hours – when the collected data is sent to the external analytics engine. |

11 Click **OK** to save the management setting overrides.

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Management Firmware

To override the access point profile's firmware upgrade settings:

1 Select **Management → Firmware**.

The management Firmware upgrade setting configuration screen displays.

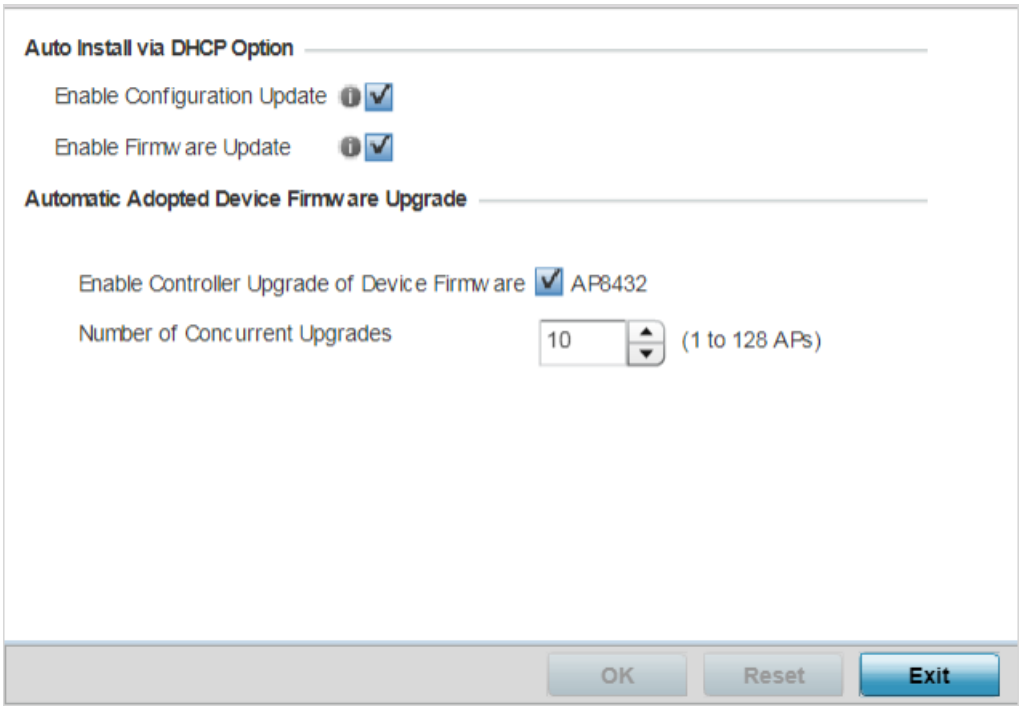



**Figure 246: Management - Firmware Upgrade Configuration Screen**

2 Refer to the Auto Install via DHCP Option field to configure automatic configuration file and firmware updates.

| | |
|---|---|
| Enable Configuration Update | Select this option to enable automatic configuration file updates for the controller profile from a location external to the access point. |
| Enable Firmware Update | Select this option to enable automatic firmware updates for this profile from a user-defined remote location. This value is disabled by default. |

3 In the Automatic Adopted Device Firmware Upgrade section, define an automatic firmware upgrade from a local file.

| | |
|---|---|
| Enable Controller Update of Device Firmware | Select the access point model to upgrade using its associated Virtual Controller AP's most recent firmware file for that model. This parameter is enabled by default. |
| Number of Concurrent Upgrades | Use the spinner control to define the maximum number (1 - 128) of adopted APs that can receive a firmware upgrade at the same time. Keep in mind that during a firmware upgrade, the access point is offline and unable to perform its normal client support role until the upgrade process is complete.<br><br>Note:<br>This is applicable in case the access point is a virtual controller. |

4 Click **OK** to save the management firmware overrides.

Click **Reset** to revert to the last saved configuration.

**Profile Overrides - Management Heartbeat**

To override the access point profile's management heartbeat configuration:

1 Select **Managemt → Heartbeat**.

The management Heartbeat setting configuration screen displays.

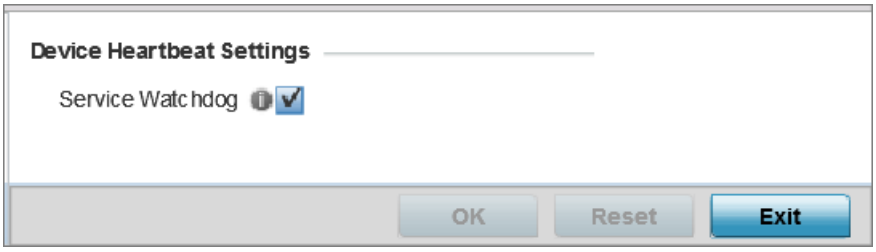



**Figure 247: Managemnet - Heartbeat Configuration Screen**

2 Select the **Service Watchdog** option to implement heartbeat messages.

This ensures that associated devices are up and running and can interoperate effectively. The Service Watchdog is enabled by default.

3 Click **OK** to save the changes and overrides made to the profile's configuration.

Click **Reset** to revert to the last saved configuration.

*Profile Overrides - Meshpoint*

An access point can be configured to be a part of a meshed network. A mesh network is one where nodes in the network can communicate with each where each node can maintain more than one path to its peers. Mesh networking enables users to access broadband applications anywhere, including moving vehicles, by providing robust, reliable, and redundant connectivity to all the members of the network. When one of the nodes in a mesh network becomes unavailable, the other nodes in the network can still communicate with each other directly or through intermediate nodes.

*Mesh point* is the name given to a device that is a part of a meshed network.

Use the Mesh Point screen to configure or override the parameters that set how this device behaves as a part of the mesh network.

Note

WiNG 7.1 release does not provide MeshConnex support on AP505 and Ap510 model access points. This feature will be supported in future releases.

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides** and select **Meshpoint**.

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

The Meshpoint main screen displays.

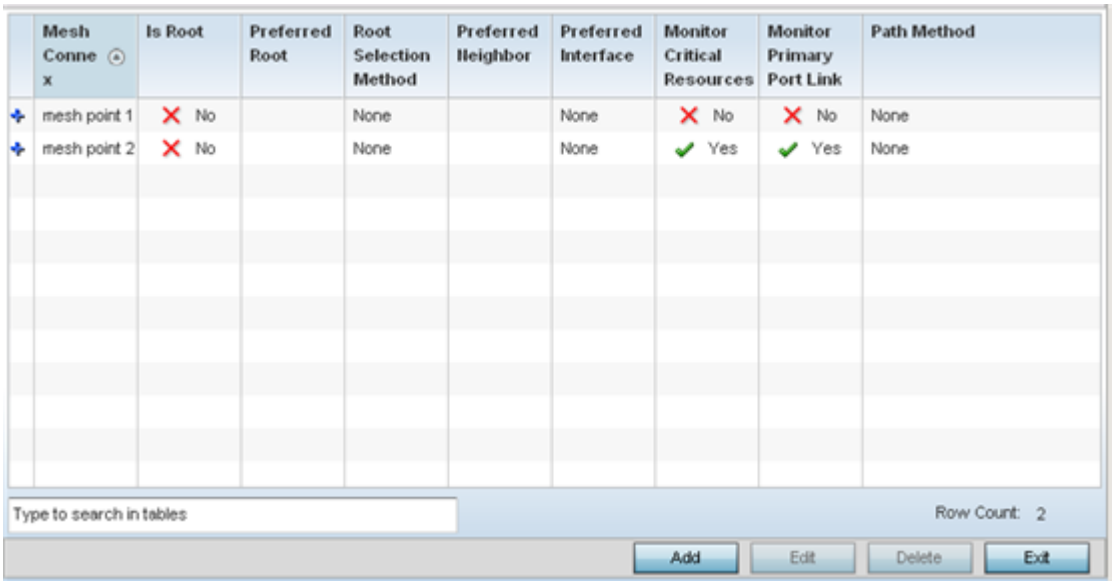



**Figure 248: Profile Overrides - Meshpoint - Main Screen**

4 To modify or override an existing meshpoint settings, click **Edit**.

To create a new meshpoint, click **Add**. If necessary, existing configurations can be selected and permanently removed by clicking **Delete**.

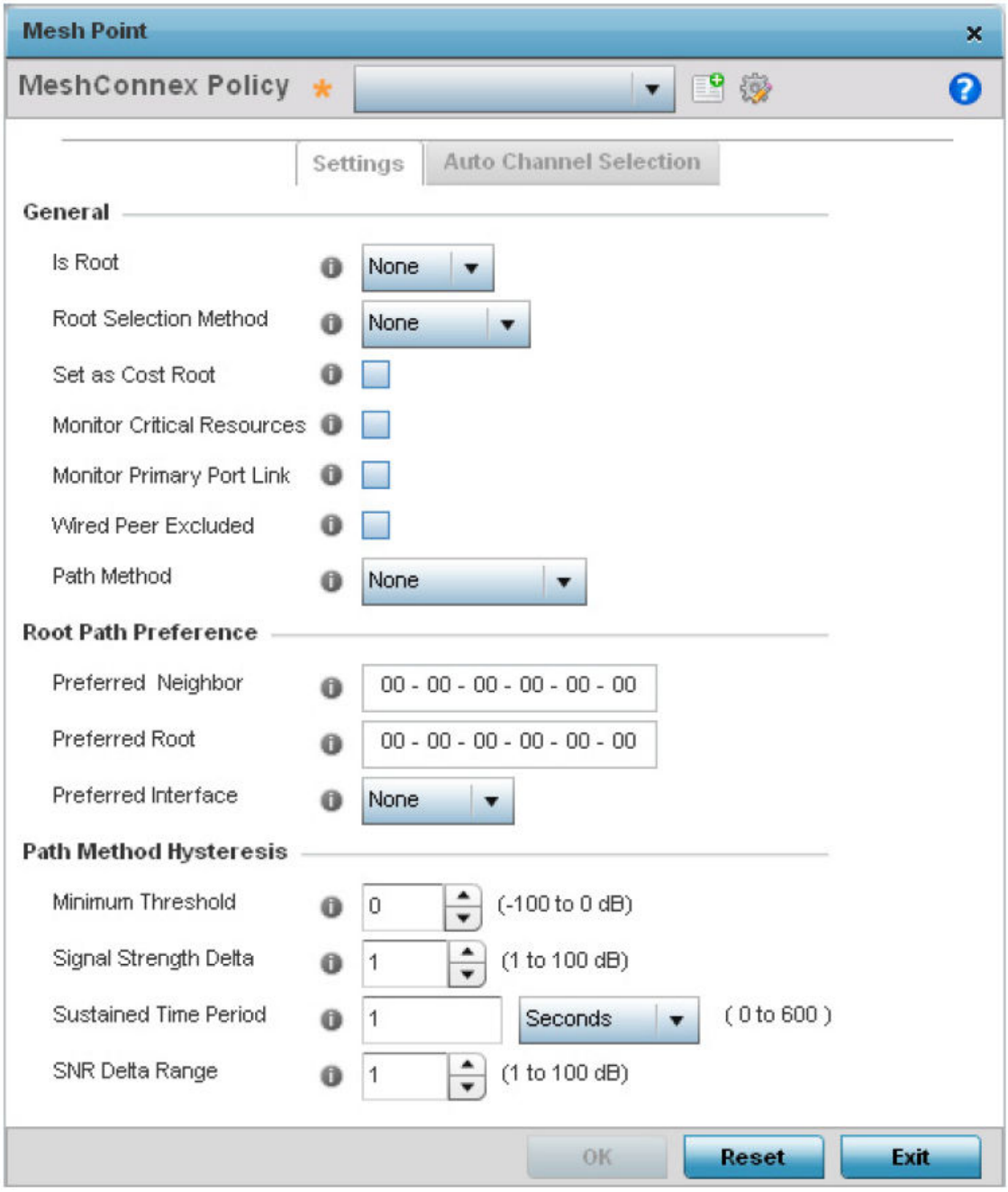



**Figure 249: Mesh Point Settings Screen**

5 Define the following General mesh point settings:

| | |
|---|---|
| MeshConnex Policy | Provide a name for the Mesh Connex Policy. Use the **Create** icon to create a new Mesh Connex Policy. To edit an existing policy, select it from the drop-down and click the **Edit** icon. For more information on creating or editing a Mesh Connex Policy, see MeshConnex Policies on page 646. |
| Is Root | Select the root behavior of this access point. **`True`** means that this access point is a root node for this mesh network, and **`False`** means that it is not a root node.<br>A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. |
| Root Selection Method | Use the drop-down menu to determine whether this mesh point is the root or non-root mesh point. Select either **`None`** (the default setting) or **`auto-mint`**. |
| Set as Cost Root | Select this option to set the mesh point as the cost root for mesh point root selection. This setting is disabled by default. |
| Monitor Critical Resources | Select this option to enable critical resource monitoring for this mesh point. |
| Monitor Primary Port Link | Select to enable monitoring of primary port link is enabled for this mesh connex policy. If the primary port link is not present and if the device is a mesh root, it is automatically changed to a non-root device. When the primary port link becomes available again, the non-root device is changed back to a root device. |
| Path Method | Select the method used for path selection in a mesh network. Available options include:<br>• **`None`** – No criteria are used in root path selection.<br>• **`uniform`** – The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths).<br>• **`mobile-snr-leaf`** – The access point is mounted on a vehicle or a mobile platform (WiNG models only). The path to the route is selected based on the SNR *(Signal To Noise Ratio)* with the neighbor device.<br>• **`snr-leaf`** – The path with the best signal to noise ratio is always selected.<br>• **`bound-pair`** – Select this option to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied. |

Note

An AP 7161 model access point can be deployed as a VMM *(vehicular mounted modem)* to provide wireless network access to a mobile vehicle such as a car or train. A VMM provides layer 2 mobility for connected devices. VMM does not provide layer 3 services, such as IP mobility. For VMM deployment considerations, see Vehicle Mounted Modem (VMM) Deployment Considerations on page 278.

6 Set the following Root Path Preference values:

| | |
|---|---|
| Preferred Neighbor | Specify the MAC address of a preferred neighbor for this mesh point. |
| Preferred Root | Specify the MAC address of a preferred mesh root for this mesh point. |
| Preferred Interface | Select the preferred Interface for this mesh point. Select **None** to set no preferences. The other interface choices are 2.4 GHz and 5 GHz. |

7 Set the following Path Method Hysteresis:

| | |
|---|---|
| Minimum Threshold | Enter the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered for selection. This field along with Signal Strength Delta and Sustained Time Period are used to dynamically select the next hop in a dynamic mesh network. The default setting is 0 dB. |
| Signal Strength Delta | Enter a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR value that is higher than the value configured here. This field along with the Minimum Threshold and Sustained Time Period are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 dB. |
| Sustained Time Period | Enter the duration (in seconds or minutes) for the duration a signal must sustain the constraints specified in the **Minimum Threshold** and **Signal Strength Delta** path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 second. |
| SNR Delta Range | Select the root selection method hysteresis (from 1 - 100dB) SNR delta range a candidate must sustain. The default setting is 1 dB. |

8 Click **OK** to save changes made to the mesh point configuration.

Click **Reset** to revert to the last saved configuration.

### ACL - Dynamic Root Selection Configuration

1 Click the **Auto Channel Selection** tab to configure the parameters for the MeshConnex Auto Channel Selection policy.

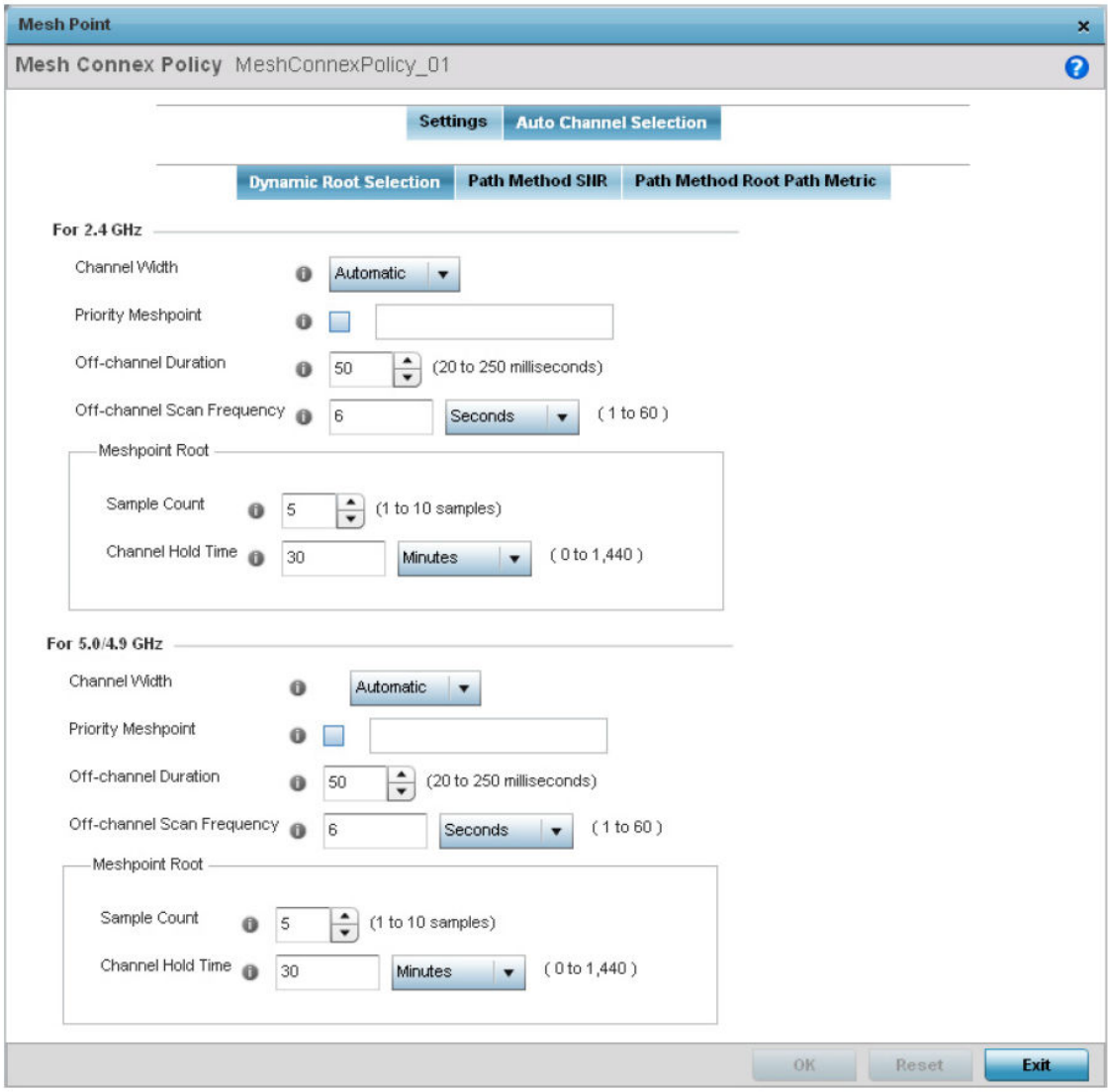



**Figure 250: Mesh Point Auto Channel Selection Screen - Dynamic Root Selection Tab**

The Dynamic Root Selection screen displays by default. This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies.

2 Refer to the following for more information on the **Auto Channel Selection → Dynamic Root Selection** screen. These descriptions are common for configuring the 2.4 GHZ and 5.0/4.9 GHz frequencies.

| | |
|---|---|
| Channel Width | Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include:<br>• **`Automatic`** – The channel width is calculated automatically. This is the default value.<br>• **`20 MHz`** – Sets the width between adjacent channels as 20 MHz.<br>• **`40 MHz`** – Sets the width between adjacent channels as 40 MHz. |
| Priority Meshpoint | Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. |
| Off-channel Duration | Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds. |
| Off-channel Scan Frequency | Set the duration (from 1- 60 seconds) between two consecutive off channel scans. The default is 6 seconds. |
| Meshpoint Root: Sample Count | Configure the number of scan samples (from 1- 10) for data collection before a mesh channel is selected. The default is 5. |
| Meshpoint Root: Channel Hold Time | Configure the duration (from 0 - 1440 minutes) to remain on a channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default setting is 30 minutes. |

3 Click **OK** to save the changes made to the mesh point configuration.

Click **Reset** to revert to the last saved configuration.

### ACL - Path Method SNR Configuration

1 Select the **Path Method SNR** tab to configure SNR ratio values when selecting the path to the meshpoint root.

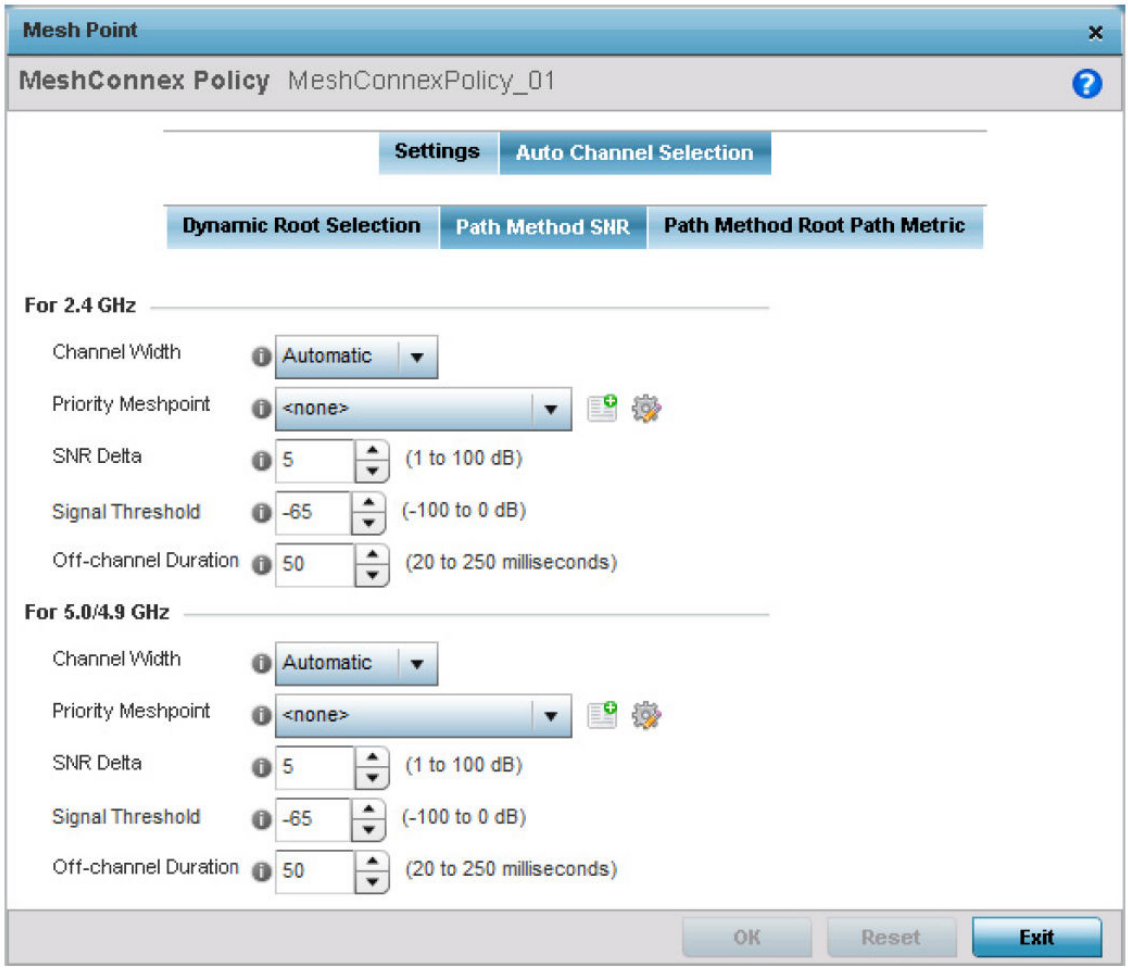



**Figure 251: Mesh Point Auto Channel Selection Screen - Path Method SNR Tab**

2 Set the following for both **2.4 GHz** and **5.0/4.9 GHz**:

| | |
|---|---|
| Channel Width | Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include:<br>• **`Automatic`** – The channel width is calculated automatically. This is the default value.<br>• **`20 MHz`** – Sets the width between adjacent channels as 20 MHz.<br>• **`40 MHz`** – Sets the width between adjacent channels as 40 MHz. |
| Priority Meshpoint | Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. |

| | |
|---|---|
| SNR Delta | Set the SNR ratio delta (from 1 - 100 dB) for mesh path selections.<br>When path selection occurs, the defined value is utilized for selecting the optimal path. A better candidate, on a different channel, must have a signal strength that exceeds this delta value when compared to the signal strength of the next hop in the mesh network. The default setting is 5 dB. |
| SNR Threshold | Set the SNR threshold for mesh path selections (from -100 to 0 dB).<br>If the signal strength of the next mesh hop falls below this set value, a scan is triggered to select a better next hop. the default setting is -65 dB. |
| Off-channel Duration | Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds. |

3 Click **OK** to save the changes made to the mesh point configuration.

Click **Reset** to revert to the last saved configuration.

### ACL - Path Method Root Path Metric Configuration

1 Select the **Path Method Root Path Metric** tab to calculate root path metrics.

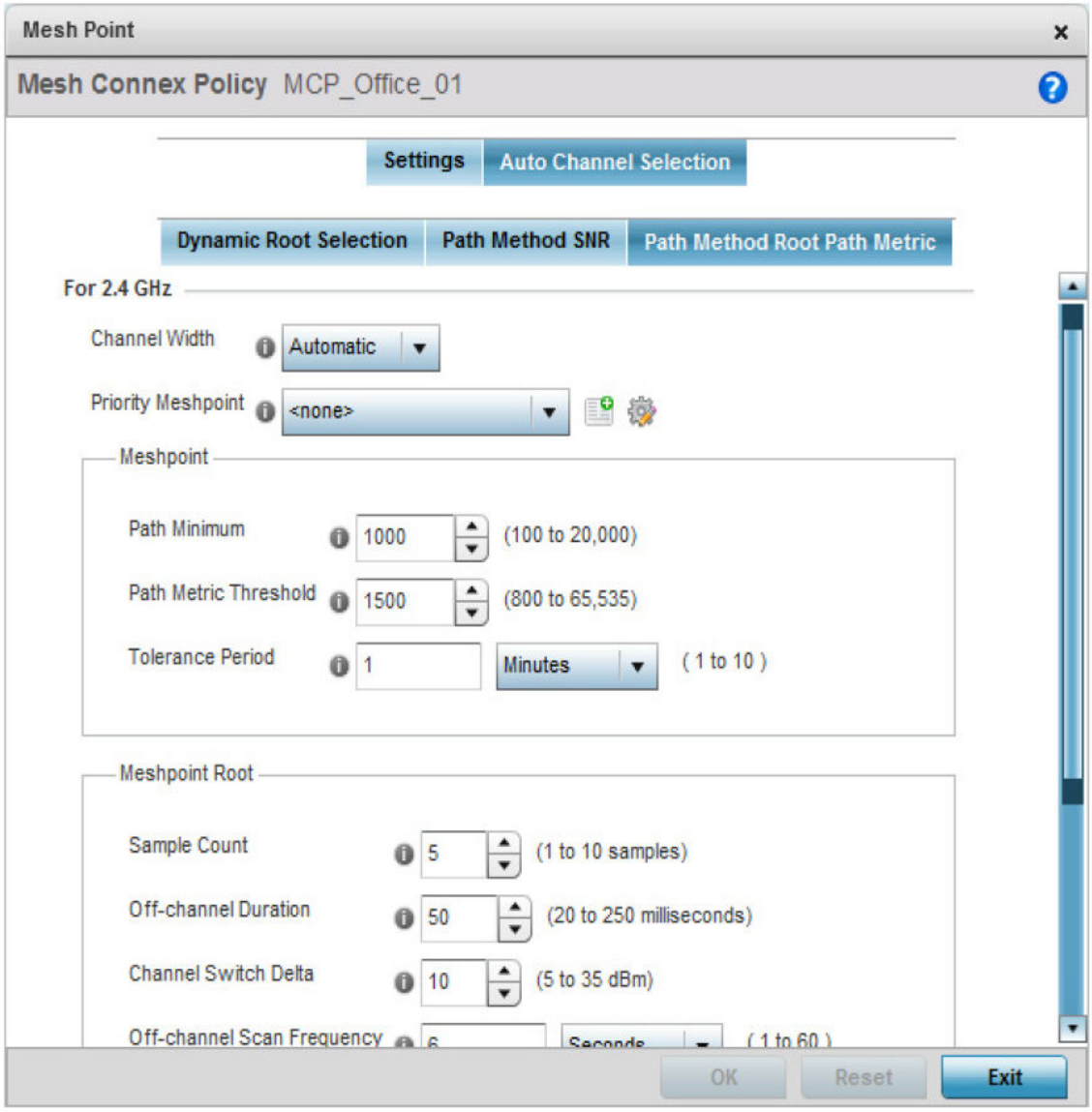



**Figure 252: Mesh Point Auto Channel Selection Screen - Path Method Root Path Metric Tab**

2 Set the following Path Method Root Path Metric values.

These descriptions apply to both the **2.4 GHz** and **5.0/4.9 GHz** frequencies.

| | |
|---|---|
| Channel Width | Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include:<br>• **Automatic** – The channel width is calculated automatically. This is the default value.<br>• **20 MHz** – Sets the width between adjacent channels as 20 MHz.<br>• **40 MHz** – Sets the width between adjacent channels as 40 MHz. |
| Priority Meshpoint | Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. |
| Meshpoint: Path Minimum | Set the minimum path metric (from 100 - 20,000) for establishing mesh connections. The default setting is 1000. |
| Meshpoint: Path Metric Threshold | Configure a minimum threshold (from 800 - 65535) for triggering an automatic channel selection for meshpoint selection. The default is 1500. |
| Meshpoint: Tolerance Period | Configure the duration to wait before triggering an automatic channel selection for the next hop. The default is 1 minute. |
| Meshpoint Root: Sample Count | Set the number of scans (from 1- 10) for data collection before a mesh point root is selected. The default is 5. |
| Meshpoint Root: Off-channel Duration | Configure the duration (from 20 - 250 milliseconds) that the scan dwells on each channel when performing an off-channel scan. The default is 50 milliseconds. |
| Meshpoint Root: Channel Switch Delta | Configure the delta (from 5 - 35 dBm) that triggers a meshpoint root automatic channel selection when exceeded. The default is 10 dBm. |
| Meshpoint Root: Off-channel Scan Frequency | Configure the duration (from 1 -60 seconds) between two consecutive off channel scans for meshpoint root. The default is 6 seconds. |
| Meshpoint Root: Channel Hold Time | Set the minimum duration (from 0 - 1440 minutes) to remain on a selected channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default is 30 minutes. |

3 Click **OK** to save the changes made to the mesh point configuration.

Click **Reset** to revert to the last saved configuration.

*Profile Overrides - Advanced Client Load Balancing*

Advanced device settings sets or overrides a profile's MiNT and/or NAS configurations.

MINT secures controller profile communications at the transport layer. Using MINT, a device can be configured to only communicate with other authorized (MINT enabled) devices. access point managed devices can communicate with each other exclusively over a MINT security domain. Keys can also be generated externally using any application (like openssl). These keys must be present on the managed device managing the domain for key signing to be integrated with the UI. A MAP device that needs to communicate with another first negotiates a security context with that device. The security context contains the transient keys used for encryption and authentication. A secure network requires users to know about certificates and PKI. However, administrators do not need to define security parameters for access points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MiNT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed.

The profile database on the RADIUS server consists of user profiles for each connected NAS *(Network Access Server)* port. Each profile is matched to a username representing a physical port. When users are authorized, it queries the user profile database using a username representative of the physical NAS port making the connection.

To set or override the client load balancing configuration at the device level:

1 Go to **Configuration → Devices → Device Overrides**.

The Device Overrides screen displays. This screen lists devices within the managed network.

2 Select an access point.

The selected access point's configuration menu displays.

3 Expand **Profile Overrides → Advanced**.

The Client Load Balancing screen displays by default.

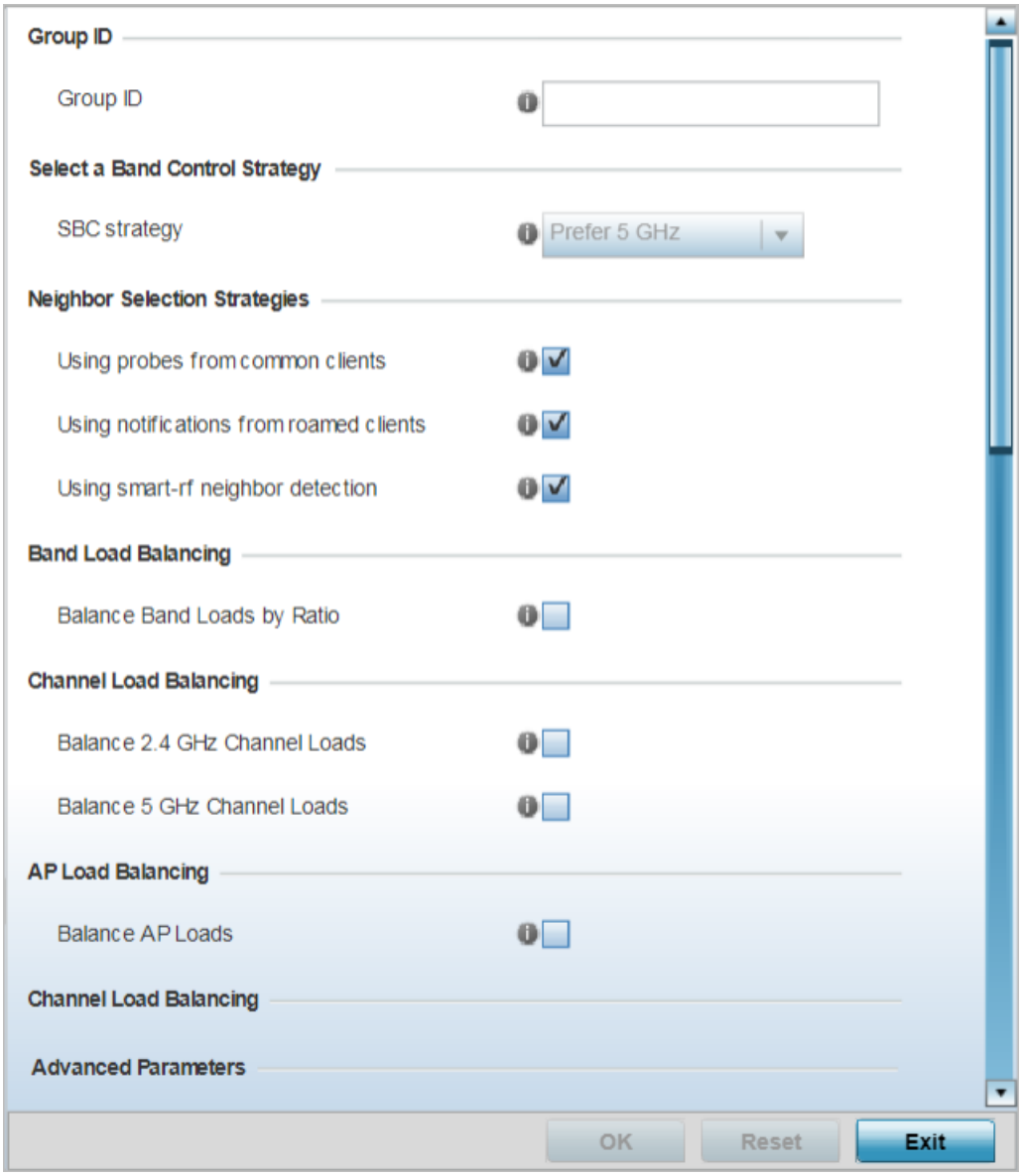



**Figure 253: Porifle Overrides - Advanced - Client Load Balancing Configuration Screen**

4 Use the Group ID field to define a group ID of up to 32 characters.

5 Use the **SBC strategy** drop-down menu to determine how band steering is conducted.

Options include **`Prefer 5GHz`**, **`Prefer 2.4 GHz`** and **`distribute-by-ratio`**. The default value is **`Prefer 5GHz`**.

6 Set the following **Neighbor Selection Strategies**:

| | |
|---|---|
| Using Probes from common clients | Select this option to select neighbors (peer devices) using probes from common clients. This option is enabled by default. |
| Using Notifications from roamed clients | Select this option to select neighbors (peer devices) using roam notifications from roamed clients. This option is enabled by default. |
| Using smart-rf neighbor detection | Select this option to select neighbors (peer devices) using the Smart RF neighbor detection algorithm. This option is enabled by default. |

7 Enable **Balance Band Loads by Ratio**, in the **Band Load Balancing** field, to distribute an access point's client traffic load across both the 2.4 and 5 GHz radio bands.

8 Configure the following **Channel Load Balancing** settings:

| | |
|---|---|
| Balance 2.4 GHz Channel Loads | Select this option to balance the access point's 2.4GHz radio load across the channels supported in the country of deployment. This can prevent congestion on the 2.4GHz radio if a channel is overutilized. |
| Balance 5 GHz Channel Loads | Select this option to balance the access point's 5GHz radio load across the channels supported in the country of deployment. This can prevent congestion on the 5GHz radio if a channel is overutilized. |

9 Enable **Balance AP Loads**, in the **AP Load Balancing** field, to distribute client traffic evenly among neighbor access points.

AP loads are balanced by assigning a ratio to both the 2.4 and 5GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 or 5 GHz band.

10 Set the following **Advanced** parameters:

| | |
|---|---|
| Max. 2.4 GHz Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points. |
| Min. Value to Trigger 2.4 Ghz Channel Balancing | Define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 2.4GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70%. |
| Weightage given to Client Count | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Increase this value if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%. |
| Weightage given to Throughput | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Increase this value if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%. |
| Max. 5 GHz Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing 5 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points. |
| Min. Value to Trigger 5 Ghz Channel Balancing | Define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 5GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70% |

| | |
|---|---|
| Weightage given to Client Count | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Increase this value if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%. |
| Weightage given to Throughput | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%. |

11 Define the following **AP Load Balancing** settings:

| | |
|---|---|
| Min. Value to Trigger Load Balancing | Set the access point radio threshold value (from 0 - 100%) used to initiate load balancing across other access point radios. When this radio load exceeds the defined threshold, load balancing is initiated. The default is 70%. |
| Max. AP Load Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing access point radio load balances. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing access point radio load balances. |
| Weightage given to Client Count | Assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Increase this value if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%. |
| Weightage given to Throughout | Assign a weight (between 0 - 100) the access point uses to prioritize throughput in the access point load calculation. Increase this value if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%. |

12 Set the following **Band Control** values:

| | |
|---|---|
| Max. Band Load Difference Considered Equal | Set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 and 5GHz radio band load balances on this access point. The default setting is 10%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing 2.4 and 5 GHz load balances on this access point. |
| Band Ratio (2.4 GHz) | Set a loading ratio (between 0 - 10) the access point 2.4 GHz radio uses in respect to radio traffic load on the 2.4 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz radio band. The higher this value is set, the greater the weight assigned to radio traffic load on the 2.4 GHz radio band. The default setting is 1. |
| Band Ratio (5 GHz) | Set a loading ratio (between 0 - 10) the access point 5 GHz radio uses in respect to radio traffic load on the 5 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 5 GHz radio band. The higher this value is set, the greater the weight assigned to radio traffic load on the 5 GHz radio band. The default setting is 1. |
| 5 GHz load at which both bands enabled | Set a load percentage (between 0 - 100) that enables the other band (2.4 GHz) to share load with the current band. |
| 2.4 GHz load at which both bands enabled | Set a load percentage (between 0 - 100) that enables the other band (5 GHz) to share load with the current band. |

13 Define the following Neighbor Selection settings:

| | |
|---|---|
| Minimal signal strength for common clients | Set the minimum signal strength require to learn about neighbors from clients that are common with the neighbor access point. |
| Minimum number of clients seen | Set the minimum number of common clients seen before the neighbor is learned. |
| Max confirmed neighbors | Set the maximum number of learned neighbors stored at this device. |
| Minimum signal strength for smart-rf neighbors | Set the minimum signal strength of neighbor devices that are learned through Smart RF before being recognized as neighbors. |

14 Click **OK** to save the changes made to the profile's advanced client load balance configuration

Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Advanced MiNT Protocol

To set or override MiNT Protocol related configurations at the device level:

1 Select **MINT Protocol**.

The MiNT Settings tab displays by default.

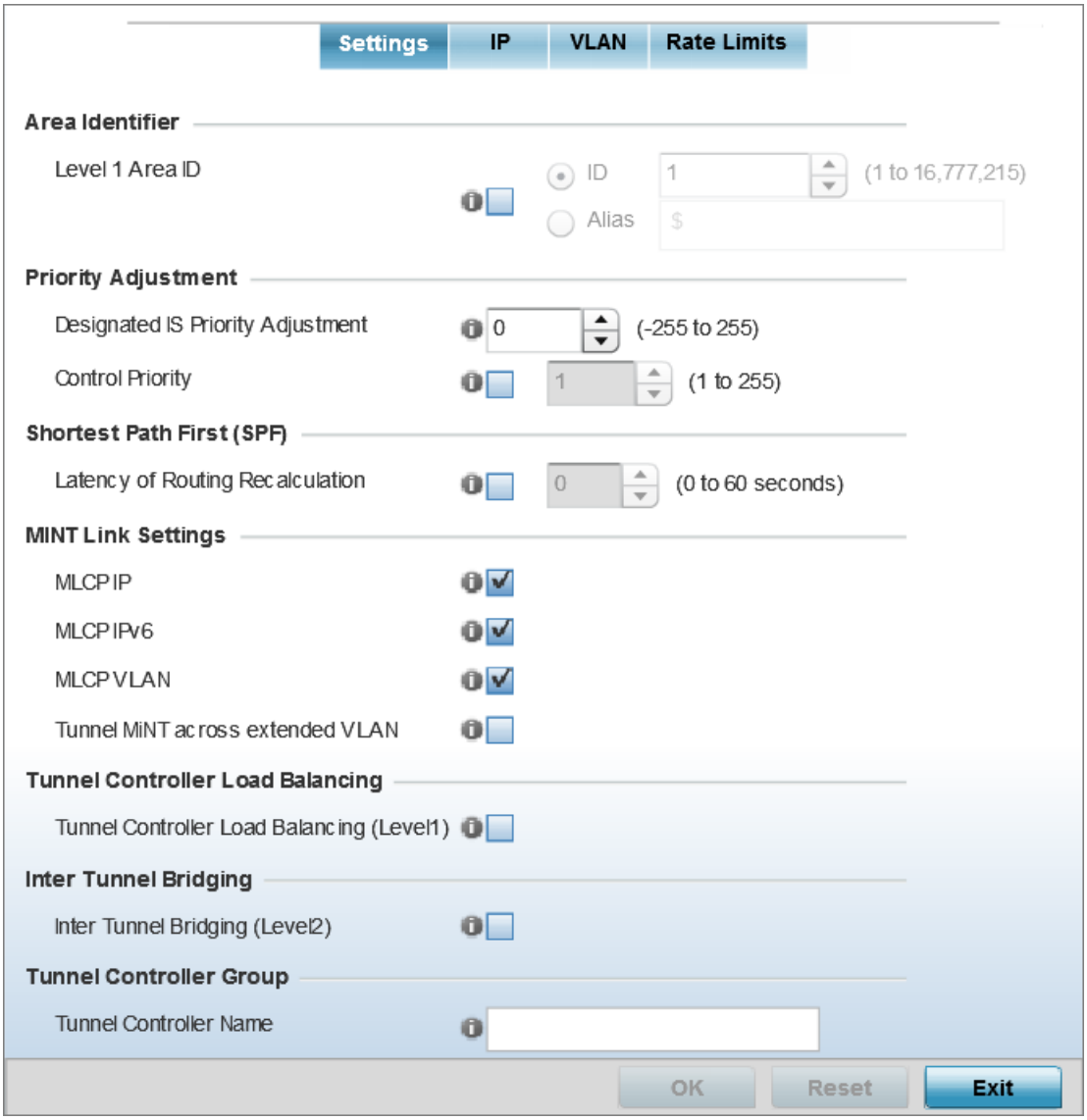



**Figure 254: Profile Overrides - Advanced MiNT Settings Configuration Screen**

2 In the Area Identifier field, define or override the Level 1 and Level 2 Area IDs used by the profile's MiNT configuration.

| | |
|---|---|
| Level 1 Area ID | Select this option to enable a spinner control for setting the Level 1 Area ID from 1 - 16,777,215. The default value is disabled. Alternatively, provide an alias by selecting the **`Alias`** option and adding the alias name to this field. |

3 In the **Priority Adjustment** field, set or override the following settings:

| | |
|---|---|
| Designated IS Priority Adjustment | Use the spinner control to set a Designated IS Priority Adjustment setting from -255 - +255. This is the value added to the base level DIS priority to influence the DIS *(Designated IS)* election. A value of +1 or greater increases DISiness. The default setting is 0. |
| Control Priority | Select to set the priority of this device with respect to others, within the network, in being selected as the Level 2 router. Higher the value, higher is the chances of the device of becoming the Level 2 router.<br>Note:<br>This option is disbaled by default. |

4 In the Shortest Path First (SPF) field, select the **Latency of Routing Recalculation** option to enable the spinner control used for defining or overriding a latency period (from 0 - 60 seconds).

The option is disabled by default.

5 Define or override the following MiNT Link Settings:

| | |
|---|---|
| MLCP IP | Select this option to enable MLCP *(MiNT Link Creation Protocol)* by IP Address. MLCP is used to create a UDP/IP link from the device to a neighbor.<br>The neighboring device can be another AP.<br>Note:<br>This option is enabled by default. |
| MLCP IPv6 | Select this option to enable MLCP by IPv6 Address. MLCP by IPv6 is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a virtual controller; it can be an standalone access point.<br>Note:<br>This option is enabled by default. |
| MLCP VLAN | Select this option to enable MiNT MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor.<br>The neighboring device can be another AP.<br>Note:<br>This option is enabled by default. |
| Tunnel MiNT across extended VLAN | Select this option to tunnel MiNT protocol packets across an extended VLAN.<br>Note:<br>This option is disabled by default. |

6 Select **Tunnel Controller Load Balancing (Level 1)** to enable load balancing through a WLAN tunnel controller.

This option is disabled by default.

7 In the Inter Tunnel Bridging field, select **Inter Tunnel Bridging (Level 2)** to enable inter tunnel bridging.

This option is disabled by default.

8 In the Tunnel Controller Group field, enter a 64-character maximum `Tunnel Controller Name` for this tunneled-WLAN-controller interface.

9 In the Preferred Tunnel Controller Group field,

a Enter the group name of clustered tunnel controllers in the Preferred Tunnel Controller Name field.

b Click the **Re-elect Tunnel Controller for this AP** button to re-elect a different tunnel controller.

This is specific for this access point only.

10 Click **OK** to save the changes made to the MiNT protocol configuration.

Click **Reset** to revert to the last saved configuration.

11 Select the **IP** tab to display the link IP network address information shared by the devices managed by the MiNT configuration.

The IP tab displays the IP address, Routing Level, Listening Link, Port, Forced Link, Link Cost, Hello Packet Interval, Adjacency Hold Time, IPSec Secure, and IPSec GW information that managed devices use to communicate securely with each other.

The MiNT IP configuration screen displays.

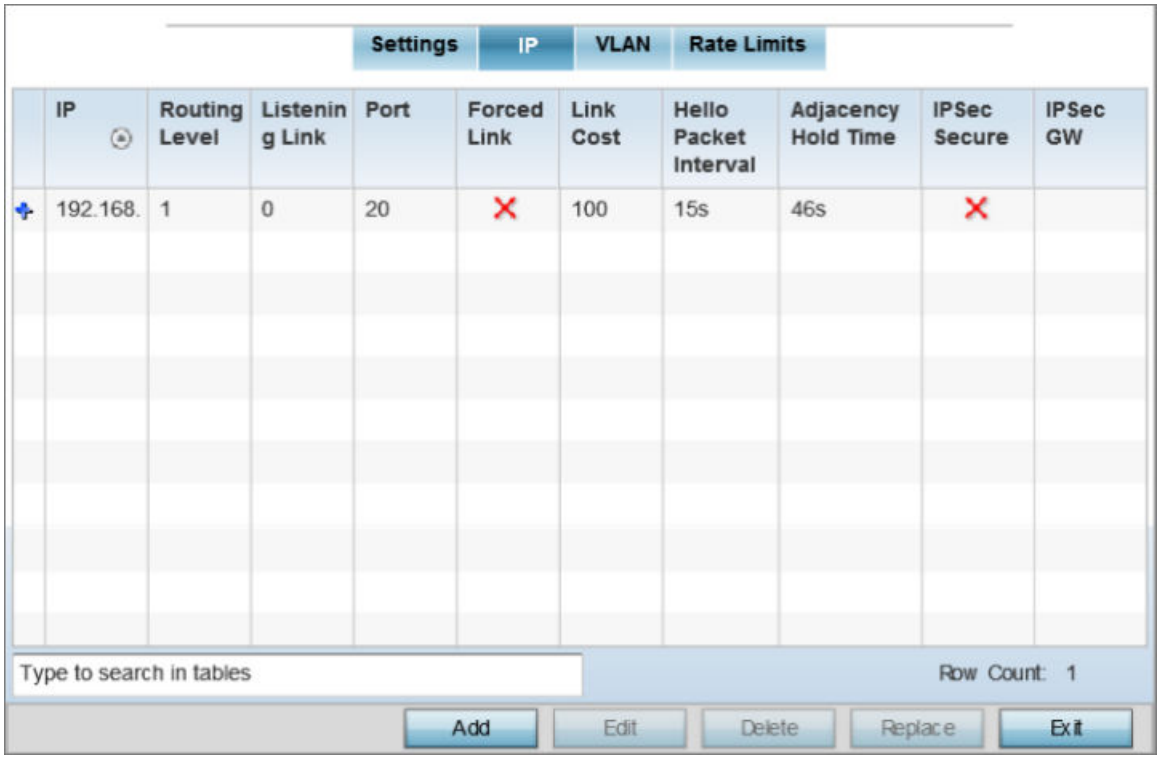



**Figure 255: Profile Overrides - Advanced - MiNT - IP Configuration Screen**

12 Click **Add** to create a new link IP configuration or **Edit** to override an existing configuration.

The add/edit MiNT IP configuration window displays.

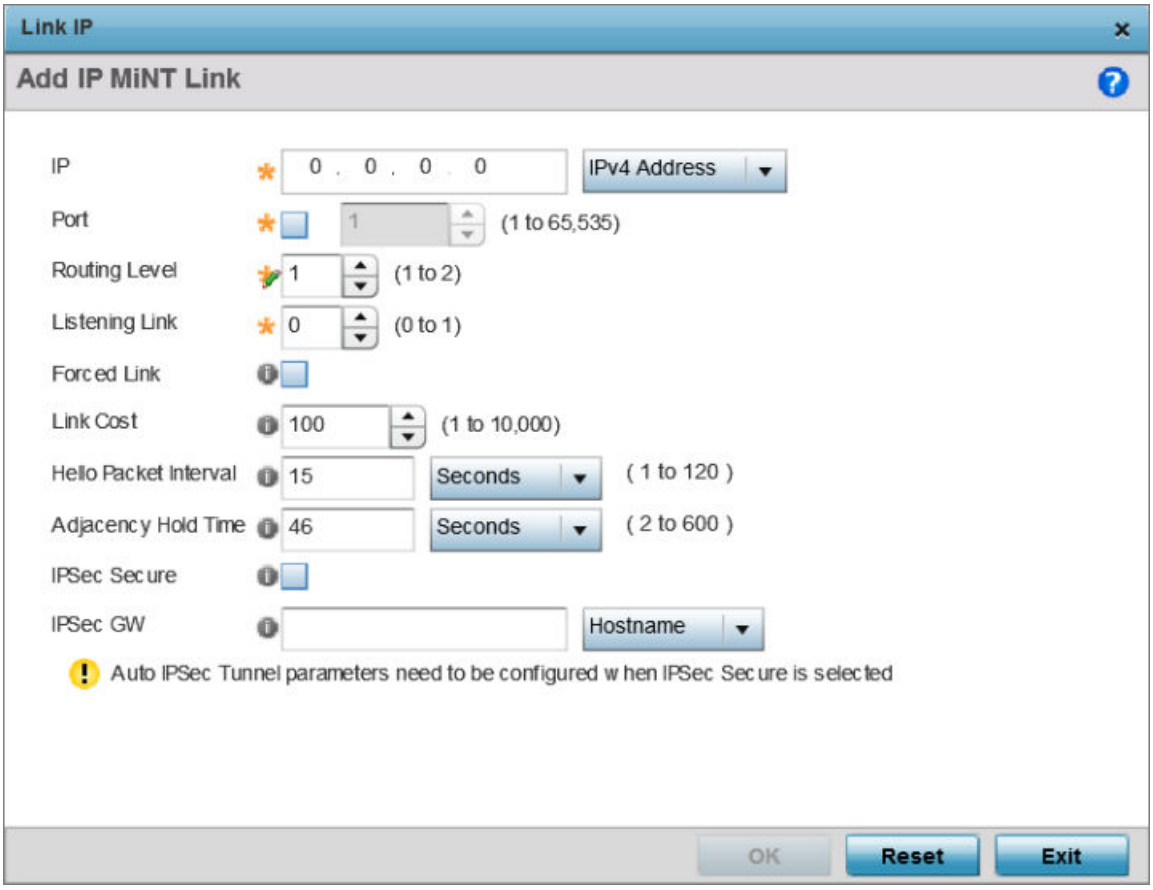



**Figure 256: Profile Overrides - Advanced - MiNT - Add IP MiNT Link**

13 Set the following Link IP parameters for the MiNT network address configuration:

| | |
|---|---|
| IP | Define or override the IP address used by peer access points for interoperation when supporting the MiNT protocol. |
| Port | To specify a custom port for MiNT links, select this option and use the spinner control to define or override the port number from 1 - 65,535. |
| Routing Level | Define or override a routing level of either 1 or 2. |
| Listening Link | Specify a listening link of either 0 or 1. UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and does not scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted. |
| Forced Link | Select this option to specify the MiNT link as a forced link.<br>Note:<br>This setting is disabled by default. |
| Link Cost | Define or override a link cost from 1 - 10,000. The default value is 100. |

| | |
|---|---|
| Hello Packet Interval | Set or override an interval in either seconds (1 - 120) or minutes (1 - 2) for the transmission of hello packets.<br><br>Note:<br>The default interval is 15 seconds. |
| Adjacency Hold Time | Set or override a hold time interval in either seconds (2 - 600) or minutes (1 - 10) for the transmission of hello packets. The default interval is 46 seconds. |
| IPSec Secure | Select this option to use a secure link for IPSec traffic. This setting is disabled by default. When this option is enabled, both the header and the traffic payload are encrypted. |
| IPSec GW | Define either an IP address or hostname for the IPSec gateway. |

14 Click **OK** to save the changes made to the MiNT protocol network address configuration.

Click **Reset** to revert to the last saved configuration.

15 Select the **VLAN** tab to display the link IP VLAN information shared by the access points managed by the MiNT configuration.

The MiNT VLAN configuration screen displays. The VLAN tab displays the VLAN, Routing Level, Link Cost, Hello Packet Interval, and Adjacency Hold Time managed devices use to communicate securely with each another.

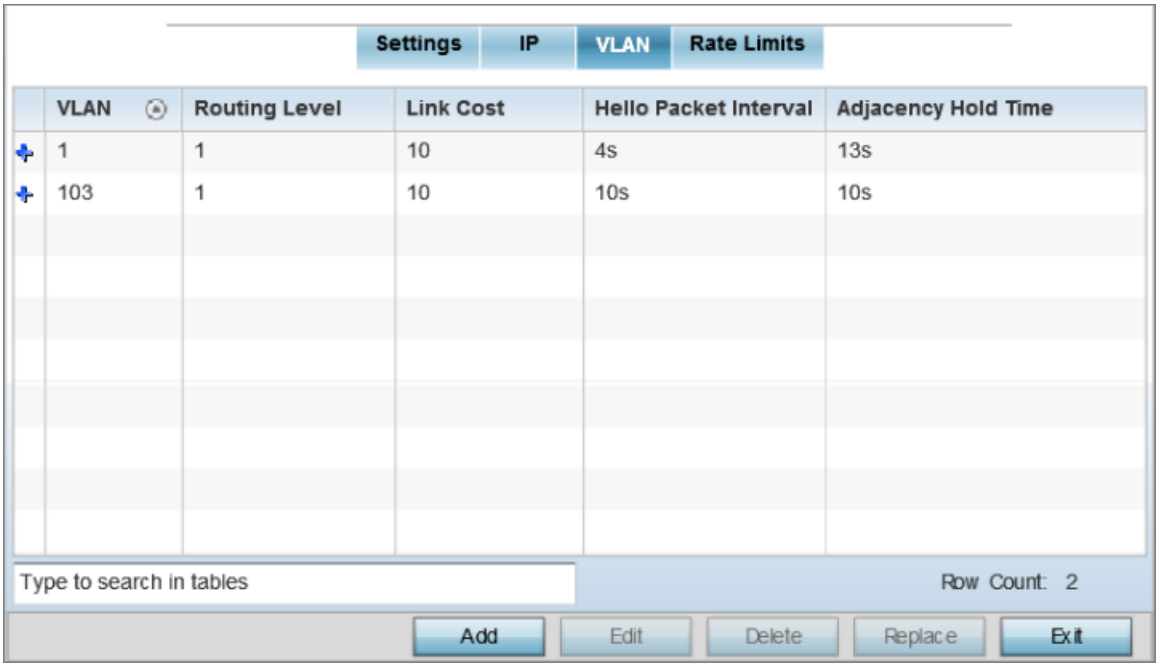



**Figure 257: Profile Overrides - Advanced - MiNT - VLAN Tab**

16 Click **Add** to create a new VLAN link configuration or **Edit** to override an existing configuration.

Note

If creating a mesh link between two access points in *Standalone AP mode*, you will need to ensure a VLAN is available to provide the necessary MiNT link between the two Standalone APs.

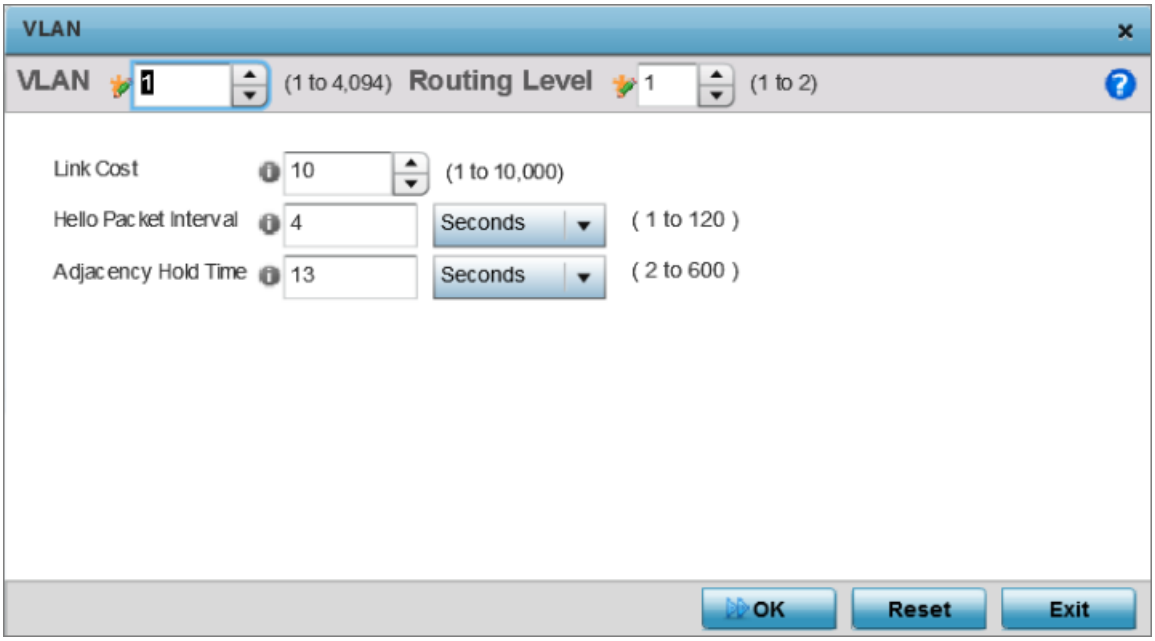



**Figure 258: Advanced Profile Overrides MiNT Screen - Add/Edit VLAN**

17 Set the following VLAN parameters for the MiNT configuration:

| | |
|---|---|
| VLAN | Define a VLAN ID from 1 - 4094 used by peer controllers for interoperation when supporting the MiNT protocol. |
| Routing Level | Define or override a routing level of either 1 or 2. |
| Link Cost | Use the spinner control to define or override a link cost from 1 - 10,000.<br>Note:<br>The default value is 10. |
| Hello Packet Interval | Set or override an interval in either seconds (1 - 120) or minutes (1 - 2) for the transmission of hello packets.<br>Note:<br>The default interval is 4 seconds. |
| Adjacency Hold Time | Set or override a hold time interval in either seconds (2 - 600) or minutes (1 - 10) for the transmission of hello packets.<br>Note:<br>p |

18 Click **OK** to save the changes made to the MiNT protocol configuration.
Click **Reset** to revert to the last saved configuration.

19 Select the **Rate Limits** tab.

The Rate Limits tab displays the Protocol, Level, Link Type, VLAN, IP, Port, Rate, Max Burst Size, Background, Best-Effort, Video, and Voice rate limiting parameters for each of the configured device.

Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices, or malicious software such as a worm or virus that has infected on one or more devices. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform, or access point are applied. An administrator can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream). Existing rate limit configurations display along with their virtual connection protocols and data traffic QoS customizations.

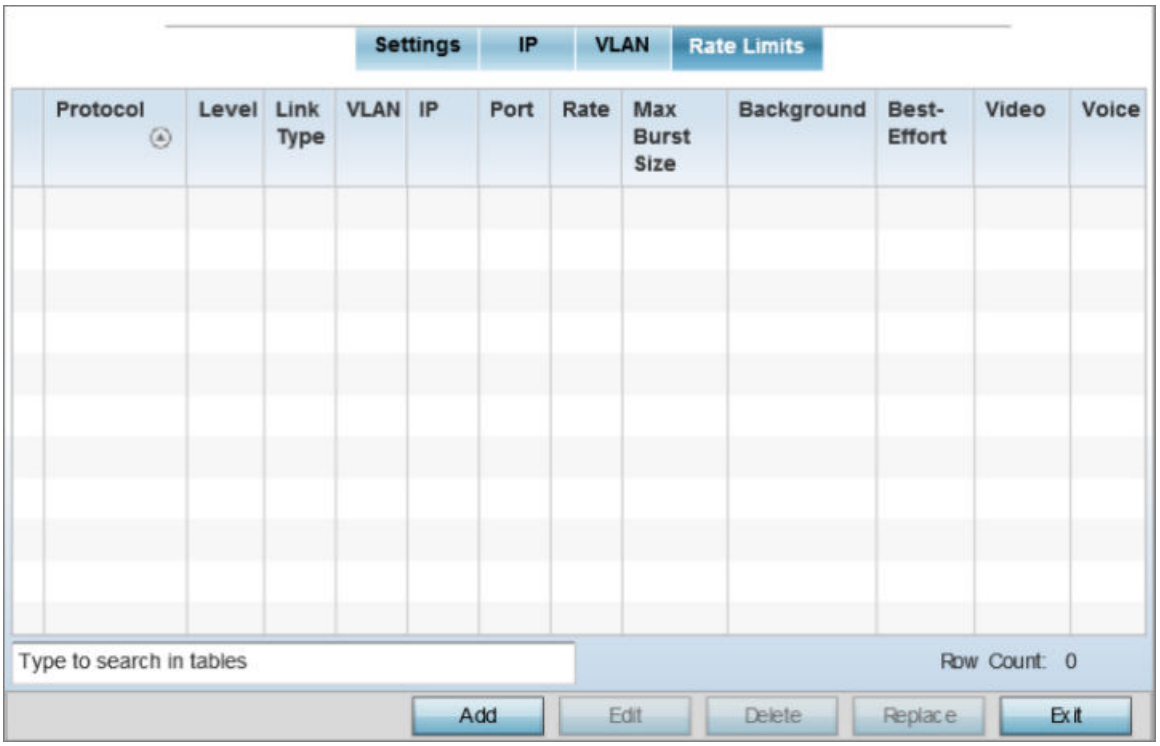



**Figure 259: Advanced Profile Overrides MiNT Screen - Rate Limits Tab**

20 Click **Add** to create a new MiNT rate limiting configuration or **Edit** to override an existing configuration.

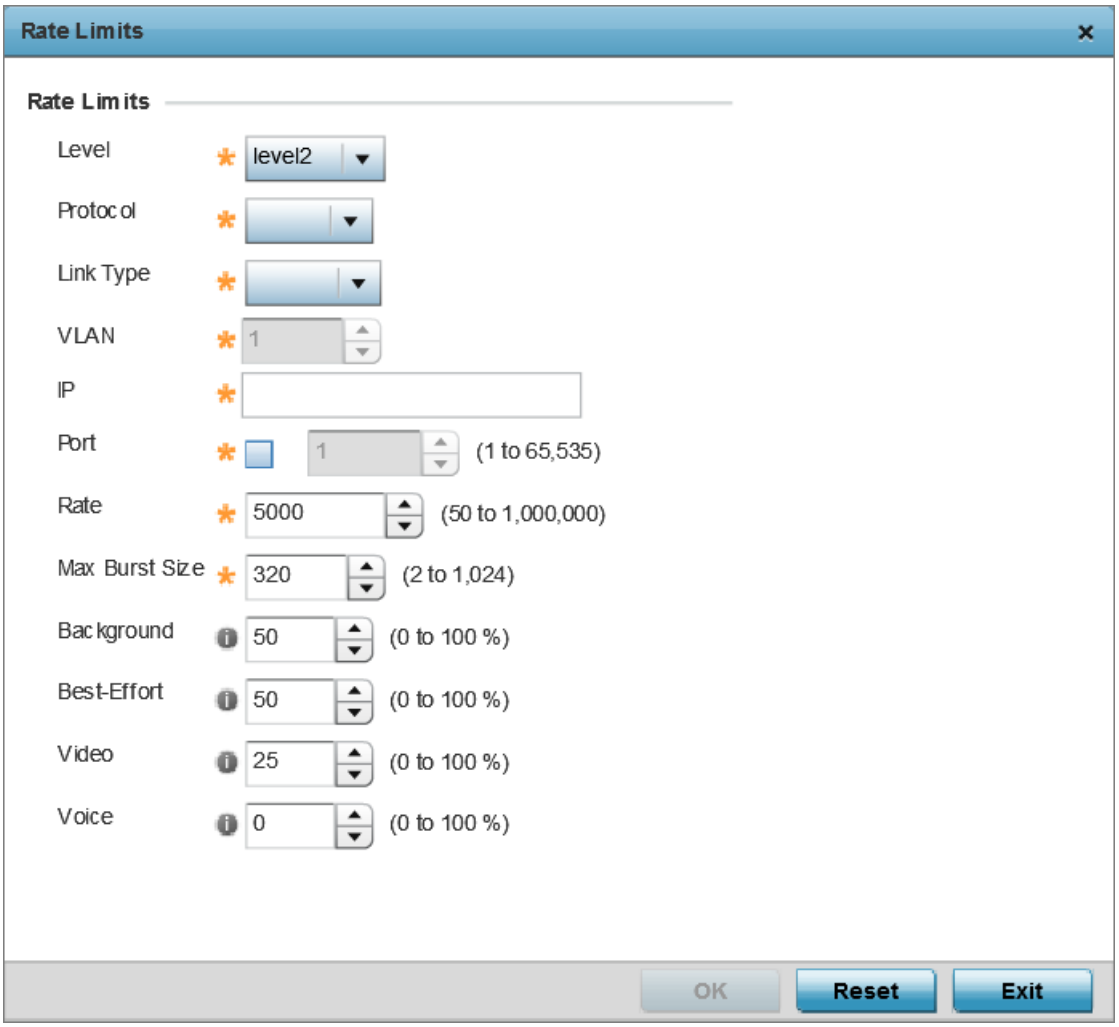



**Figure 260: Advanced Profile Overrides MiNT Screen - Add/Edit Rate Limit**

21 Set the following Rate Limits to complete the MiNT configuration:

| | |
|---|---|
| Level | Select **level2** to apply rate limiting for all links on level 2. |
| Protocol | Select either **mlcp** or **link** as this configuration's rate limit protocol. MLCP creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform; it can be an access point with a path to the controller or service platform. Select **link** to rate limit using statically configured MiNT links. |
| Link Type | Select either **VLAN**, to configure a rate limit configuration on a specific virtual LAN, or **IP** to set rate limits on a static IP address/port configuration. |
| VLAN | When **Protocol** is set to **link** and **Link Type** is set to **VLAN**, select a virtual LAN from 1 - 4094 to refine the rate limiting configuration to a specific VLAN. |
| IP | When **Protocol** is set to **link** and **Link Type** is set to **VLAN**, enter the IP address as the network target for rate limiting. |

| | |
|---|---|
| Port | When **Protocol** is set to **link** and **Link Type** is set to **VLAN**, set the virtual port (1 - 65,535) used for rate limiting traffic. |
| Rate | Define a rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated.<br><br>Note:<br>The default setting is 5000 kbps. |
| Max Burst Size | Set the maximum burst size from 0 - 1024 kb. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts.<br><br>Note:<br>The default burst size is 320 kbytes. |
| Background | Configure the random early detection threshold (as a percentage) for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).<br><br>Note:<br>The default setting is 50%. |
| Best-Effort | Configure the random early detection threshold (as a percentage) for low priority best effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).<br><br>Note:<br>The default setting is 50%. |

| | |
|---|---|
| Video | Configure the random early detection threshold (as a percentage) for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).<br><br>Note:<br>The default setting is 25%. |
| Voice | Configure the random early detection threshold (as a percentage) for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).<br><br>Note:<br>The default setting is 0%. |

22 Click **OK** to save the changes made to the MiNT protocol rate limit configuration.
Click **Reset** to revert to the last saved configuration.

### Profile Overrides - Advanced Miscellaneous

To define or override the access point profile's miscellaneous settings:

1 Select the **Advanced** → **Miscellaneous** menu item.
The miscellaneous settings configuration screen displays.

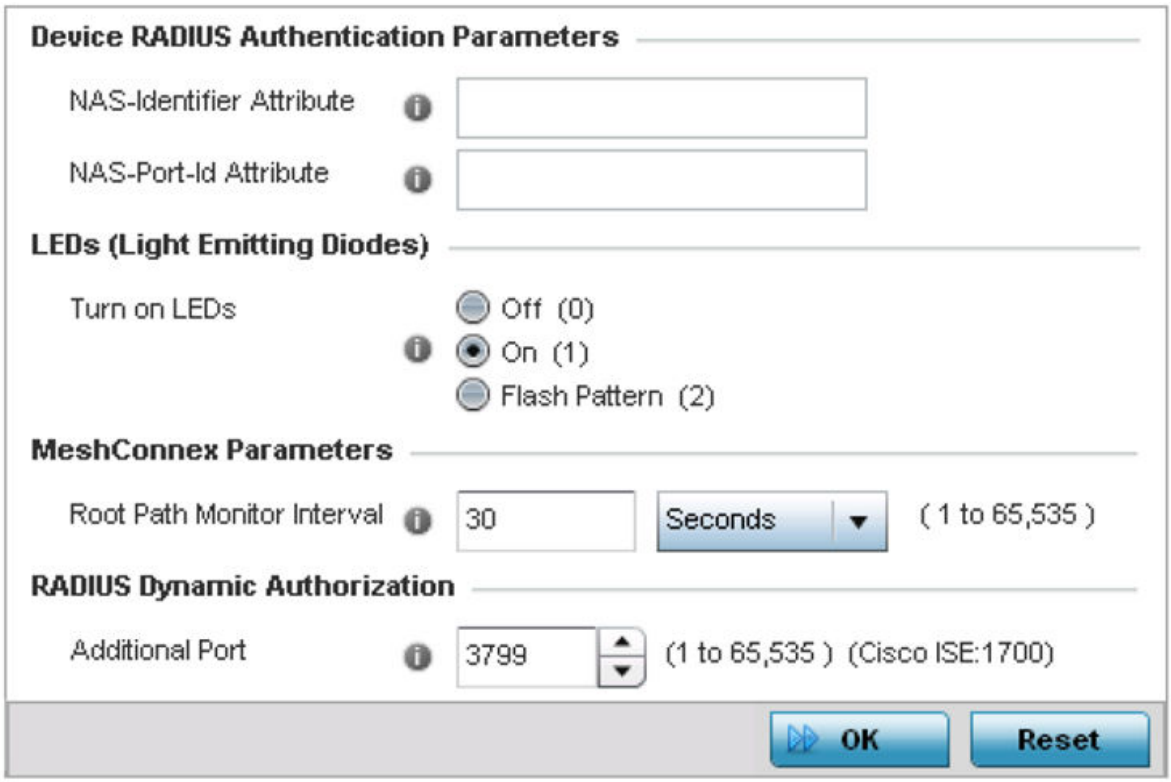



**Figure 261: Profile Overrides - Advanced - Miscellaneous Configuration Screen**

2 In the Device RADIUS Authentication Parameters field,

a Set a **NAS-Identifier Attribute** up to 253 characters in length.

This is the RADIUS NAS-Identifier attribute that typically identifies where a RADIUS message originates.

a Set a **NAS-Port-Id Attribute** up to 253 characters in length.

This is the RADIUS NAS port ID attribute which identifies the device port where a RADIUS message originates.

3 In the LEDs (Light Emitting Diodes) field, select one of the following **Turn on LEDs**option: to enable the LEDs on an access point.

- Off (0) - select to disable LEDs on the access point.
- On (1) - select to enable LEDs on an access point.

Note

This is the default setting.

- Flash Pattern (2) - to enable the access point to blink in a manner different from its operational LED behavior.

Note

Enabling this option allows an administrator to validate that the access point has received its configuration from its managing controller during staging. In the staging process, the administrator adopts the access point to a staging controller to get an initial configuration before the access point is deployed at its intended location. Once the access point has received its initial configuration, its LED blinks in a unique pattern to indicate the initial configuration is complete.

4 In the MeshConnex field, use the **Root Path Monitor Interval** option to configure the interval (from 1 - 65,535 seconds) to monitor the path to the root node. This value specifies how often to check if the mesh point is up or down.

5 In the RADIUS Dynamic Authorization section, set the **Additional Port** value to enable a Cisco *(Identity Services Engine)* AAA *(Authentication, Authorization and Accounting)* server to dynamically authenticate a client.

Set this value to 1700. The allowed port range is 1 to 65,535.

When a client device requests access to the network, the Cisco ISE RADIUS server presents the client with a URL where a device's compliance is checked for definition file validity (this form of file validity checking is called *posture*). The check verifies, for example, that the device's anti-virus or anti-spyware software is valid. If the device complies, it is allowed access to the network.

6 Click **OK** to save the changes made to the profile's advanced miscellaneous configuration.

Click **Reset** to revert to the last saved configuration.

## Auto-Provisioning Policies

Wireless devices can adopt and manage other wireless devices. For example, a wireless controller can adopt any number of access points. When a device is adopted, the device configuration is provisioned by the adopting device. Since multiple configuration policies are supported, an adopting device needs

to define which configuration policies are used for a given adoptee. Auto-provisioning policies determine which configuration policies are applied to an adoptee based its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP snoop strings, etc.

Once created an auto-provisioning policy can be used in profiles or device configuration objects. An Auto-Provisioning policy contains a set of ordered by precedence rules that either *deny* or *allow* adoption based on potential adoptee properties and a catch-all variable that determines if the adoption should be allowed when none of the rules is matched. All rules (both deny and allow) are evaluated sequentially starting with the rule with the lowest precedence. The evaluation stops as soon as a rule has been matched, no attempt is made to find a better match further down in the set.

The evaluation is performed using various matching criteria. The matching criteria supported include:

| | |
|---|---|
| MAC | Matches the MAC address of a device attempting to be adopted. Either a single MAC address or a range of MAC addresses can be specified. |
| VLAN | Matches when adoption over a Layer 2 link matches the VLAN ID of an adoption request. Note that this is a VLAN ID as seen by the recipient of the request, in case of multiple hops over different VLANs this may different from VLAN ID set by the sender. A single VLAN ID is specified in the rule. This rule is ignored for adoption attempts over Layer 3. |
| IP Address | Matches when adoption is using a Layer 3 link matches the source IP address of an adoption request. In case of NAT the IP address may be different from what the sender has used. A single IP, IP range or IP/mask is specified in the rule. This rule is ignored for adoption attempts over Layer 2. |
| Serial Number | Matches exact serial number (case insensitive). |
| Model | Matches exact model name (case insensitive). |
| DHCP Option | Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, e.g.'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag'rf-domain', if present. This value is matched against the auto provisioning policy. |
| FQDN | Matches a substring to the FQDN of a device (case insensitive). |
| CDP | Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an Access Point snooped 3 devices: controller1.extremenetworks.com, controller2.extremenetworks.com and controller3.extremenetworks.com,'controller1','extremenetworks', 'extremenetworks.com' , are examples of the substrings that will match. |
| LLDP | Matches a substring in a list of LLDP snoop strings (case insensitive). For example, if an Access Point snooped 3 devices: controller1.extremenetworks.com, controller2.extremenetworks.com and controller3.extremenetworks.com,'controller1', 'extremenetworks', 'extremenetworks.com ', are substrings match. |

Auto provisioning is the process by which access points discover controllers or service platforms available in the network, pick the most desirable controller or service platform, establish an association, optionally obtain an image upgrade and obtain its configuration.

At adoption, an access point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the Access Point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available

controller or service platform. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

Note

A device configuration does not need to be present for an auto provisioning policy to take effect. Once adopted, and the device's configuration is defined and applied by the controller or service platform, the auto provisioning policy mapping does not have impact on subsequent adoptions by the same device.

Use an auto provisioning policy to define rules for adoption of access point by wireless controllers.

To review exisiting Auto-provisioning policies:

1 Select **Configuration → Devices → Auto-Provisioning Policy**.

The Auto-Provisioning screen displays by default. This screen displays existing auto-provisioning policies. Review these policies to determine whether a new policy requires creation, or an existing policy requires edit or deletion.

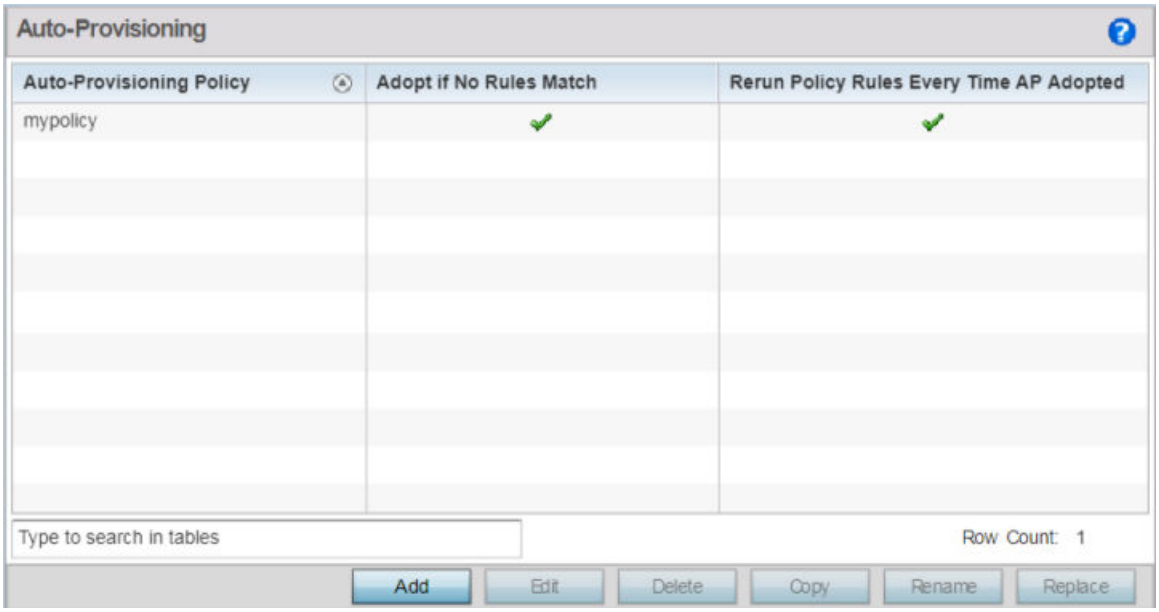



**Figure 262: Auto-Provisioning Policy Screen**

2 Review the following parameters:

| | |
|---|---|
| Auto-Provisioning Policy | Lists the name of each policy when it was created. It cannot be modified as part of the Auto-provisioning policy's edit process. |
| Adopt if No Rules Match | Displays whether this policy will adopt devices if no adoption rules apply. Doubleclick within this column to launch the edit screen where rules can be defined for device adoption. This feature is disabled by default |
| Rerun Policy Rules Every Time AP Adopted | Displays whether this policy will be run every time an AP is adopted. Double-click within this column to launch the edit screen where this option can be modified. This feature is disabled by default. |

## Configuring Auto-Provisioning Policy Rules

Auto-provisioning policies can be created or modified as unique deployment requirements dictate changes in the number of access point radios within a specific radio coverage area.

You can add a new auto-provisioning policy or edit an existing policy configuration.

1 Click **Add** to add a new policy. To modify an existing policy, select the policy from those listed on the screen and click **Edit**. To delete or replace an existing policy, select the policy and click **Delete** or **Replace** respectively.

If you are modifying an existing policy, the selected policy's Rules tab displays by default. Review the existing rules to determine whether a rule can be used as is, requires edit or whether new rules need to be defined.

The add new auto-provisioning policy screen displays.


**Figure 263: Auto-Provisioning Policy - Add New Policy Screen**

2 If adding a new auto-provisioning policy, provide a name in the Auto-Provisioning Policy field, and click **Continue**.

Note
The name must not exceed 32 characters.

The auto-provisioning policy configuration screen, with the Rules tab selected by default, displays.

3 If modifying an existing policy, the selected policy's Rules window displays by default.

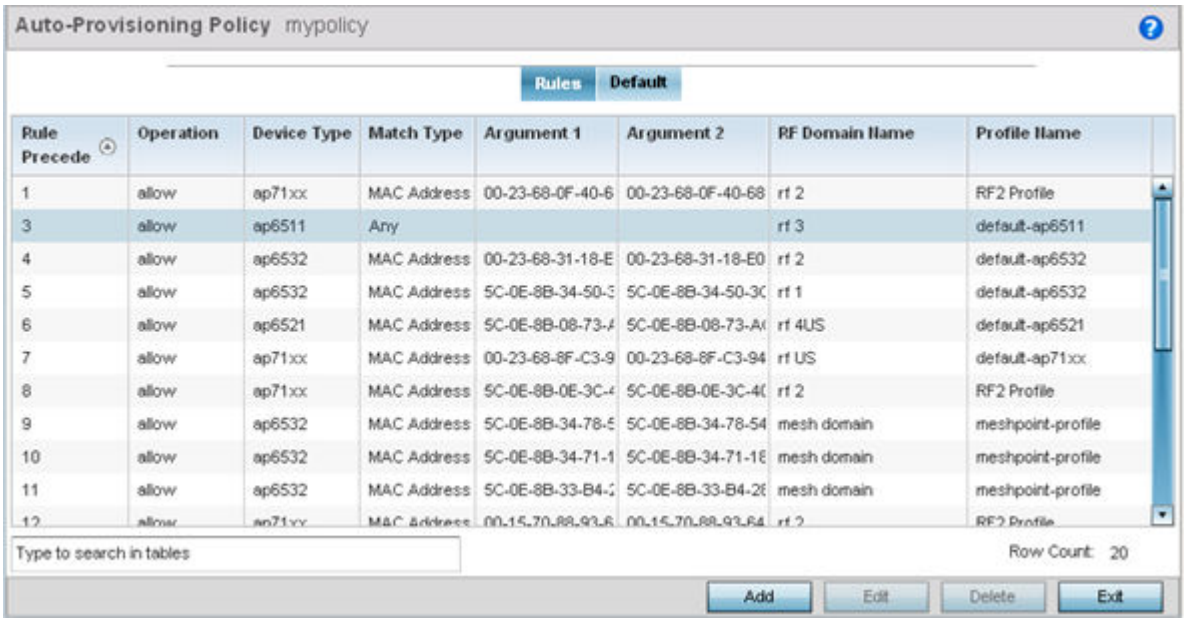



**Figure 264: Auto-provisioning Policy - Rules Tab**

4 Review the following data to determine whether a rule can be used as is, requires edit or whether new rules need to be defined:

| | |
|---|---|
| Rule Precedence | Displays the precedence (sequence) the adoption policies rules are applied. Rules with the lowest precedence receive the highest priority. This value is set (from 1 - 1000) when adding a new auto-provisioning policy rule configuration. |
| Operation | Lists the operation taken upon receiving an adoption request from an access point: The following operations are available:<br>• allow – Allows the normal provisioning of connected access points upon request.<br>• deny – Denies (prohibits) the provisioning of connected access point upon request.<br>• redirect – When selected, an access point seeks a steering controller (upon adoption request), that will forward the network credentials of a designated controller resource that initiates the provisioning process.<br>• upgrade – Conducts the provisioning of requesting access points from this controller resource. |
| Device Type | Sets the access point model for which this policy applies. Adoption rules are specific to the selected model. |

| | |
|---|---|
| Match Type | Lists the matching criteria used in the policy. This is like a filter and further refines the APs that can be adopted. The options are:<br>• MAC Address – The filter type is a MAC Address of the selected access point model.<br>• IP Address – The filter type is the IP address of the selected access point model.<br>• VLAN – The filter type is a VLAN.<br>• Serial Number – The filter type is the serial number of the selected access point model.<br>• Model Number – The filter type is the access point model number.<br>• DHCP Option – The filter type is the DHCP option value of the selected access point model. |
| Argument 1 | The number of arguments vary on the Match Type. This column lists the first argument value. This value is not set as part of the rule creation or edit process. |
| Argument 2 | The number of arguments vary on the Match Type. This column lists the second argument value. This value is not set as part of the rule creation or edit process. |
| RF Domain Name | Sets the name of the RF Domain to which the device is adopted automatically. Select the **Create** icon to define a new RF Domain configuration or select the **Edit** icon to revise an existing configuration. |
| Profile Name | Defines the name of the profile used when the auto-provisioning policy is applied to a device. Select the **Create** icon to define a new profile configuration or the **Edit** icon to revise an existing configuration. |

5 Click **Add** to add a new rule. The Rule screen displays.

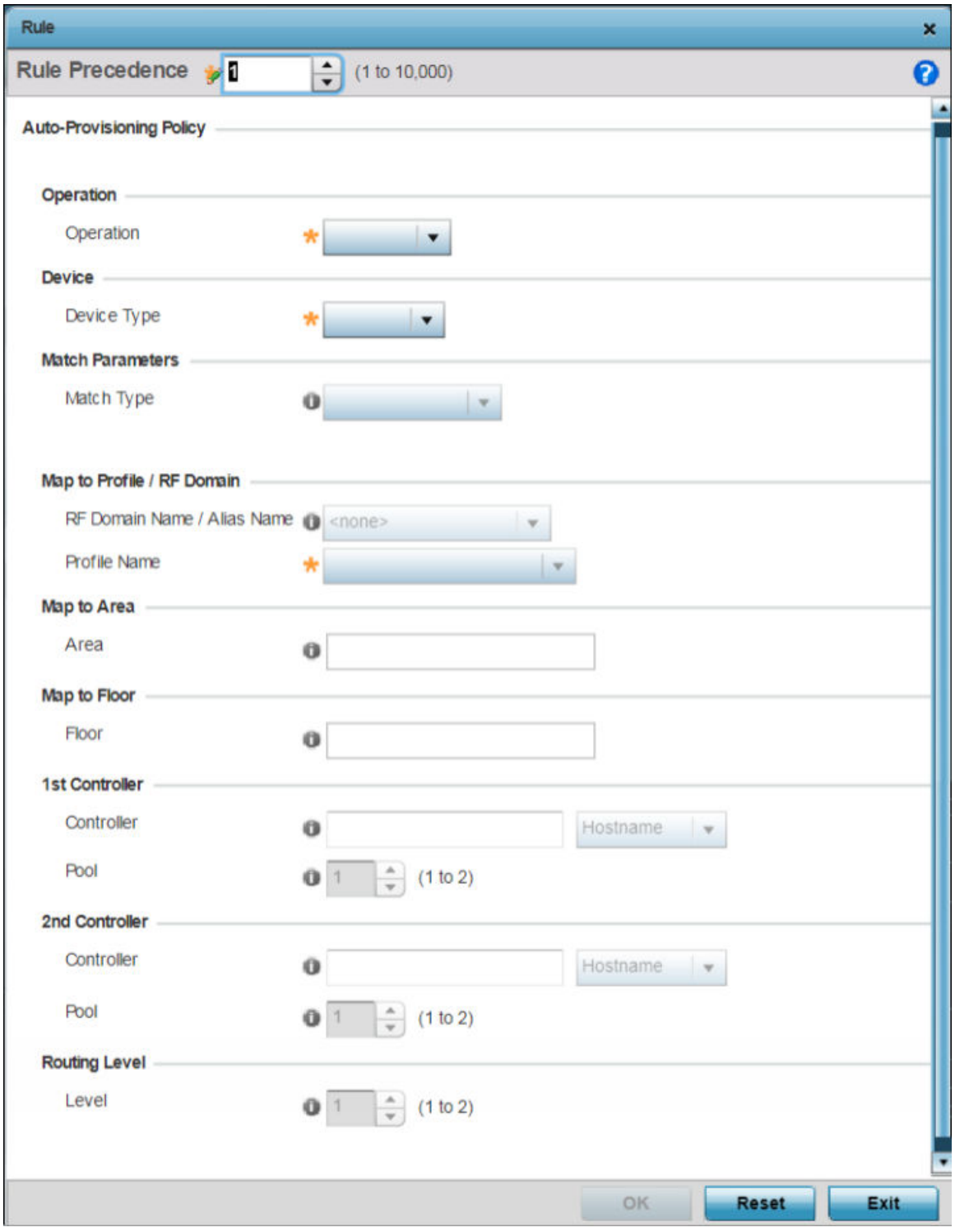



**Figure 265: Auto Provisioning Policy - Add / Edit Rule Screen**

6 Define the following parameters:

| | |
|---|---|
| Rule Precedence | Assign a priority from 1 - 10,000 for the application of the auto-provisioning policy rule. Rules with the lowest value have priority. |
| Operations | Define the operation taken upon receiving an adoption request from an access point: The following operations are available:<br>• allow – Allows the normal provisioning of connected access points upon request.<br>• deny – Denies (prohibits) the provisioning of connected access point upon request.<br>• redirect – When selected, an access point seeks a steering controller (upon adoption request), that will forward the network credentials of a designated controller resource that initiates the provisioning process.<br>• upgrade – Conducts the provisioning of requesting access points from this controller resource. |
| Device Type | Sets the access point model for which this policy applies. Adoption rules are specific to the selected model, as radio configurations are often unique to specific models. |
| Match Type | Set the matching criteria used in the policy. This is like a filter that further refines the APs that can be adopted. The options are:<br>• MAC Address – The filter type is a MAC Address of the selected access point model.<br>• IP Address – The filter type is the IP address of the selected access point model.<br>• VLAN – The filter type is a VLAN.<br>• Serial Number – The filter type is the serial number of the selected access point model.<br>• Model Number – The filter type is the access point model number.<br>• DHCP Option – The filter type is the DHCP option value of the selected access point model. |
| RF Domain Name / Alias Name | Use the RF Domain to which the device is adopted automatically. Use the drop-down menu to select the desired RF Domain from the list displayed. Alternately use an alias name to point to the RF Domain. Ensure that the alias is existing and configured. For more information on aliases, see Alias on page 708. |
| Profile Name | Define the profile used when an auto-provisioning policy is applied to a device. |
| Area | Enter a 64 character maximum deployment area name assigned to this policy. |
| Floor | Enter a 32 character maximum deployment floor name assigned to this policy. |
| 1st Controller | If you have set *Operation* to *redirect* , provide a 1st choice steering controller *Hostname / IP Address* and *pool* to forward network credentials for a controller resource to initiate the provisioning process. |
| 2nd Controller | If you have set *Operation* to *redirect* , provide a 2nd choice steering controller *Hostname / IP Address* and *pool* to forward network credentials for a controller resource to initiate the provisioning process. |
| Routing Level | If you have set *Operation* to *redirect*, specify the routing level as 1 or 2. |

7 Click **OK** to save your changes. Click **Reset** to revert to your last saved configuration.

## Configuring Auto-Provisioning Policy Adoption Criteria

To define the Auto-Provisioning Policy's rule matching adoption configuration:

1 Select the **Default** tab.

The Auto-Provisioning Default screen displays.

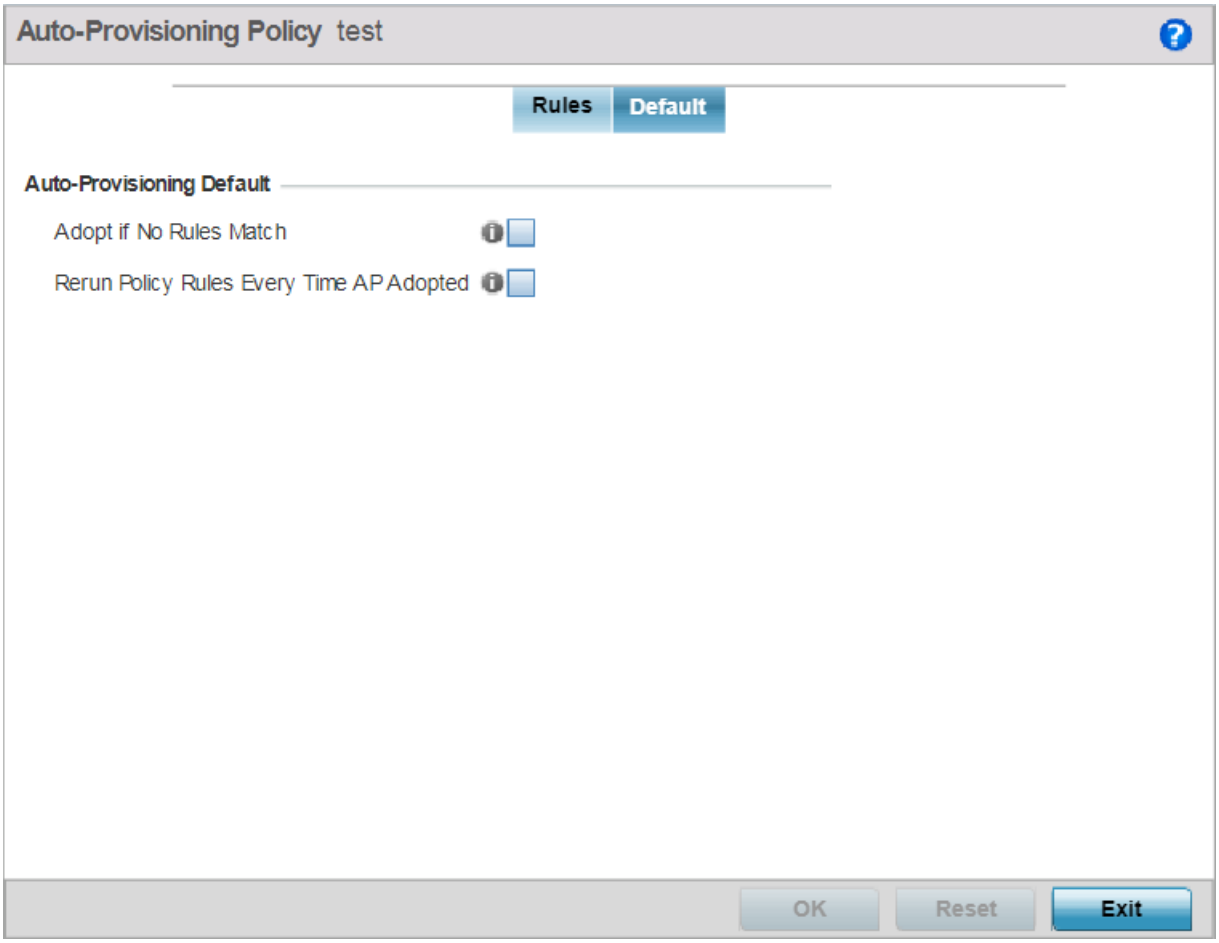



**Figure 266: Auto-provisioning Policy - Default Tab**

2 Select **Adopt if No Rules Match** to adopt when no matching filter rules apply.

This setting is disabled by default.

3 Select **Rerun Policy Rules Every Time AP Adopted** to run this policy and apply its rule set every time an access point is adopted.

This setting is disabled by default.

4 Select **OK** to save the updates to the screen.

Select **Reset** to revert the screen to the last saved configuration.

## Managing an Event Policy

Event policies enable an administrator to create specific notification mechanisms using one, some or all of the SNMP, syslog, forwarding or e-mail notification options available. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication/encryption and performance events. Once policies are defined, they can be mapped to device profiles strategically

as the likelihood of an event applies to particular devices. By default, there's no enabled event policy and one needs to be created and implemented.

Existing policies can have their event notification configurations modified as device profile requirements warrant.

To define an event policy configuration:

1 Go to **Configuration → Devices → Event Policy**.

The Event System Policy screen displays.

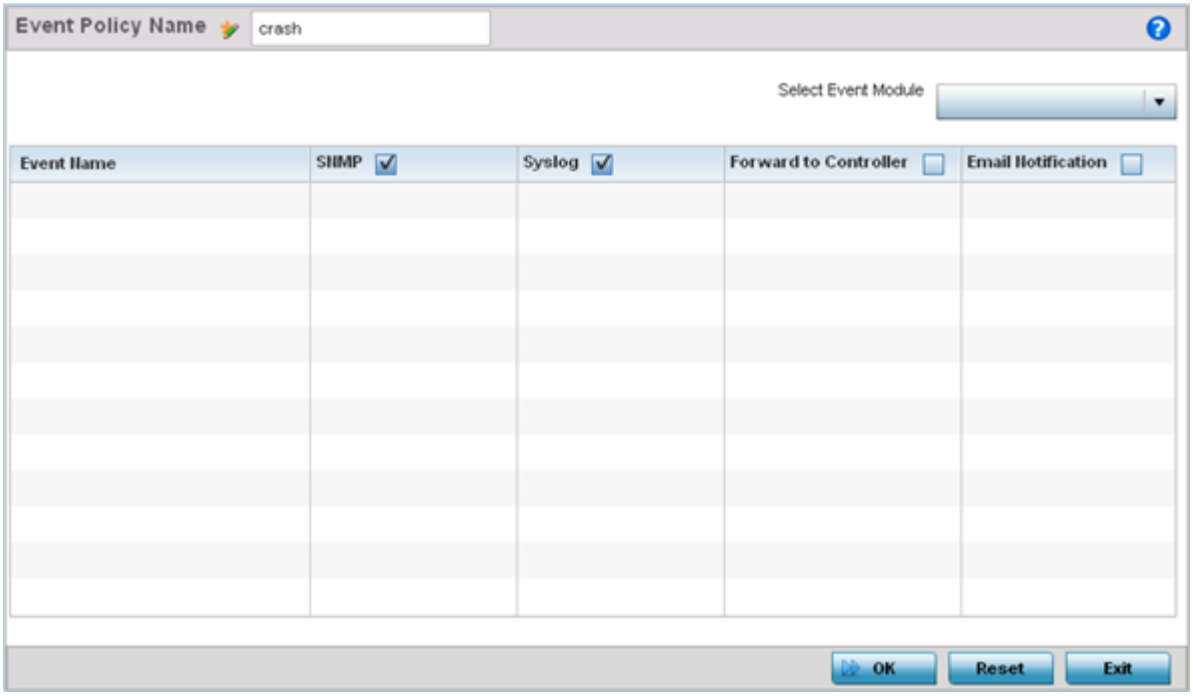



**Figure 267: Configuration - Device Configuration - Event Policy Screen**

2 Ensure the Activate Event Policy button is selected to enable the screen for configuration. This option needs to remain selected to apply the event policy configuration to the access point profile.

3 Use the **Select Event Module** drop-down menu on the top right-hand side of the screen to select an event module used to track the occurrence of each list event.

4 Review each event and select (or deselect) the **SNMP**, **Syslog**, **Forward to Switch** or **Email Notification** option as required for the event. Map an existing policy to a device profile as needed. Select Profile from the Map drop-down menu in the lower-left hand side of the screen. Expand the list of device profiles available, and apply the event policy as required.

5 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. **Delete** obsolete rows as needed.

## Password Encryption

Use this option to enable password encryption, and configure the passphrase used to encrypt passwords. When enabled, passwords configured within the system are displayed encrypted and not as clear text.

To enable pasword encryption:

1 Go to **Configuration → Devices**.

2 Select **Password Encryption**.

The Password Encryption screen displays.

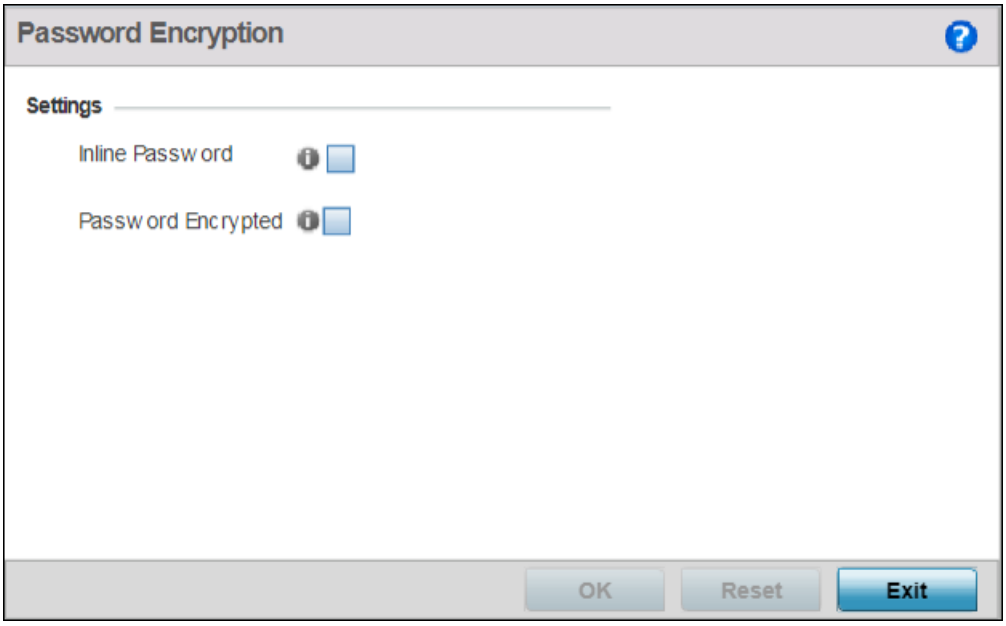



**Figure 268: Configuration - Devices - Password Encryption Screen**

3 Select the **Inline Password** option.

The inline password option moves the encryption key to the startup-config file. By default, the encryption key is not stored in the startup-config file.

4 Select the **Password Encrypted** option.

The New Password field is enabled.

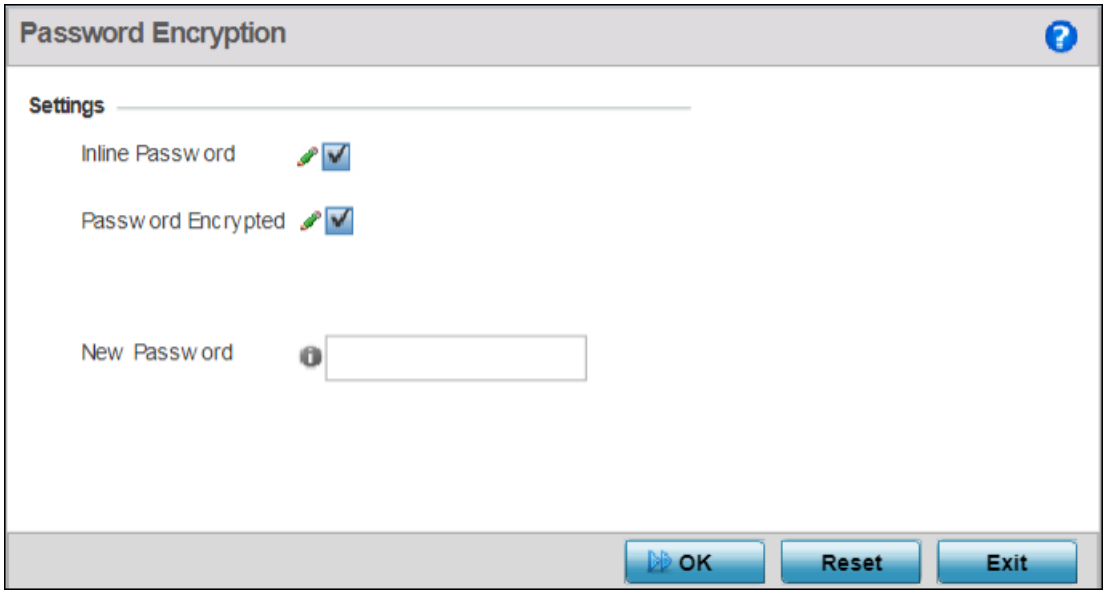



**Figure 269: Configuration - Devices - Password Encryption - New Password Field**

5 Enter the secret phrase in the New Password field. The system uses this phrase to encrypt passwords.

6 Click **OK** to save password encryption configuration.

Click **Reset** to revert to the last saved configuration.

# 7 Wireless Configuration



A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one connected access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), E-mail, file and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected access point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each connected access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to only provided service to specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

The wireless configuration is comprised the following policies:

- Wireless LAN Policies on page 551
- WLAN QoS Policies on page 604
- Radio QoS Policies on page 617
- Association ACL on page 628
- Smart RF Policies on page 631
- MeshConnex Policies on page 646
- Mesh QoS Policy on page 652

- Passpoint Policy on page 660
- Sensor Policy on page 671

WLAN policies can be separately selected and refined in the **Configuration → Wireless** pane located on the top left-hand side of the UI.

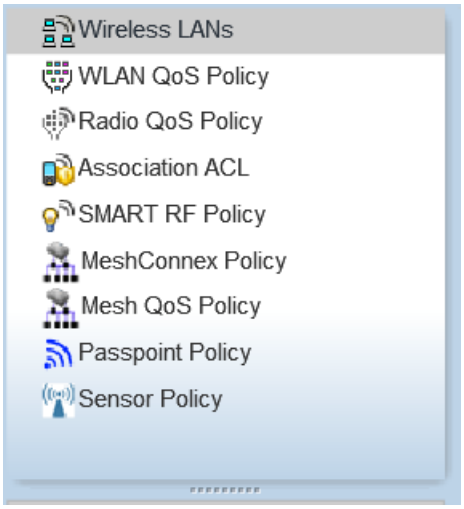



**Figure 270: Configuration > Wireless Pane**

## Wireless LAN Policies

To review the attributes of existing WLANs (policies) and, if necessary, modify their configurations:

1 Select **Configuration → Wireless → Wireless LANs** to display existing WLANs.

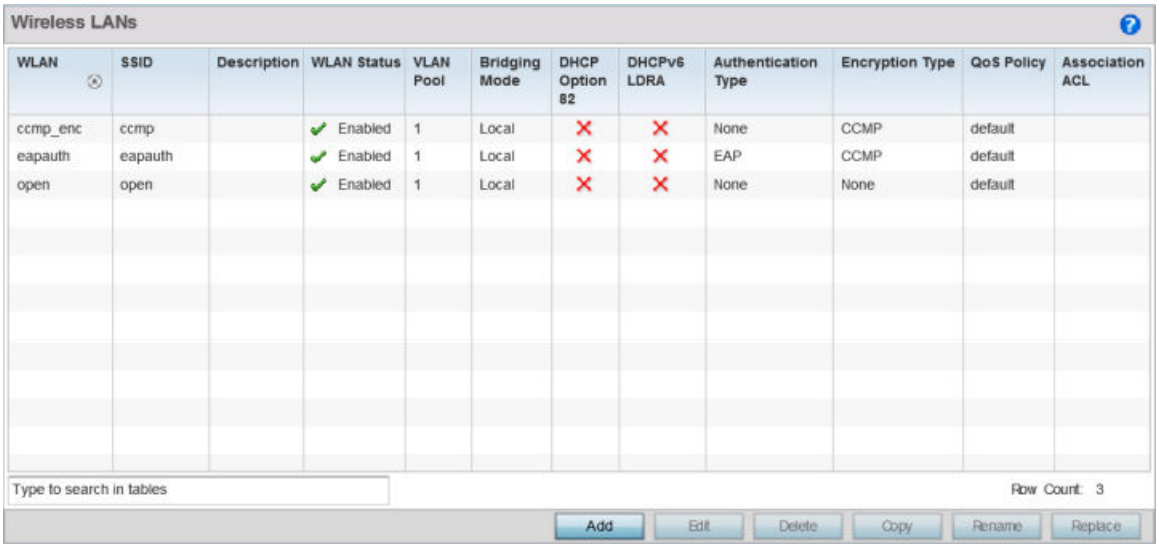



**Figure 271: Wireless LANs Screen**

2 Refer to the following (read only) information to assess the attributes of the each WLAN available:

| | |
|---|---|
| WLAN | Displays the name of each available WLAN. Individual WLANs can selected and their SSID and client management properties modified. Each access point can support up to 16 WLANs per radio. |
| SSID | Displays the SSID assigned to the WLAN when created or last modified. Optionally, select a WLAN and click **Edit** to update the WLAN's SSID. |
| Description | Displays the brief description set for each listed WLAN when it was either created or modified. |
| WLAN Status | Lists each WLAN's current status as either *Disabled* or *Enabled*. A green check mark defines the WLAN as available to clients on all radios where it has been mapped. A red "X" defines the WLAN as shutdown, meaning even if the WLAN is mapped to radios, it is not available for clients to associate. |
| VLAN Pool | Lists each WLAN's current VLAN mapping. Mapping a WLAN to more than one VLANs is permitted. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. The VLAN is picked from a pool assigned to the WLAN. Keep in mind however, typical deployments only map a single VLAN to a WLAN. The use of a pool is strictly optional. |
| Bridging Mode | Lists each WLAN's current bridging mode as either **Local** or **Tunnel**. Local infers VLAN traffic is bridged locally, Tunnel uses a shared tunnel for bridging the WLAN's VLAN traffic.<br><br>Note: The default setting is Local. |
| DHCP Option 82 | Displays whether DHCP Option 82 is enabled or not. DHCP option 82 provides additional information on the physical attachment of a client.<br><br>Note: This option is disabled by default. |
| DHCPv6 LDRA | *Lightweight DHCPv6 Relay Agent* (LDRA) is used to insert relay-agent options in DHCPv6 message exchanges that identify client-facing interfaces. These relay agents are deployed to forward DHCPv6 messages between clients and servers when they are not on the same IPv6 link. A red "X" indicates that this WLAN acts as a DHCPv6 LDRA. |
| Authentication Type | Displays the name of the user authentication scheme each listed WLAN is using to secure its client membership transmissions. *None* is listed if authentication is not used within this WLAN. Refer to the Encryption Type column if no authentication is used to verify there is some sort of data protection used with the WLAN or risk no protection at all. |
| Encryption Type | Displays the name of the encryption type each listed WLAN is using to secure its client membership transmissions. *None* is listed if encryption is not used within this WLAN. Refer to the Authentication Type column to verify that there is some sort of data protection used with the WLAN or risk using this WLAN with no protection at all. |
| QoS Policy | Lists the QoS policy applied to each listed WLAN. A QoS policy needs to be custom selected (or created) for each WLAN in respect to the WLAN's intended client traffic and the voice, video, or normal data traffic it supports. |
| Association ACL | Lists the Association ACL policy applied to each listed WLAN. An Association ACL is a policy-based *Access Control List* (ACL) that either prevents or allows connection between wireless clients and a WLAN. The mapping of an Association ACL is strictly optional. |

Use the sequential set of WLAN screens to define a unique configuration for each WLAN. Refer to the following to set WLAN configurations:



## Basic WLAN Configuration

When creating or modifying a WLAN, the Basic Configuration screen is the first screen that displays as part of the WLAN configuration screen flow. Use this screen to enable a WLAN and to and define its SSID, client behavior, and VLAN assignments.

To define a WLAN's basic configuration:

1 Select **Configuration → Wireless → Wireless LANs**.

The list of existing WLANs is displayed.

2 Select **Add** to create an additional WLAN, or select an existing WLAN then click **Edit** to modify its properties.

WLANs can also be removed as they become obsolete by selecting **Delete**.

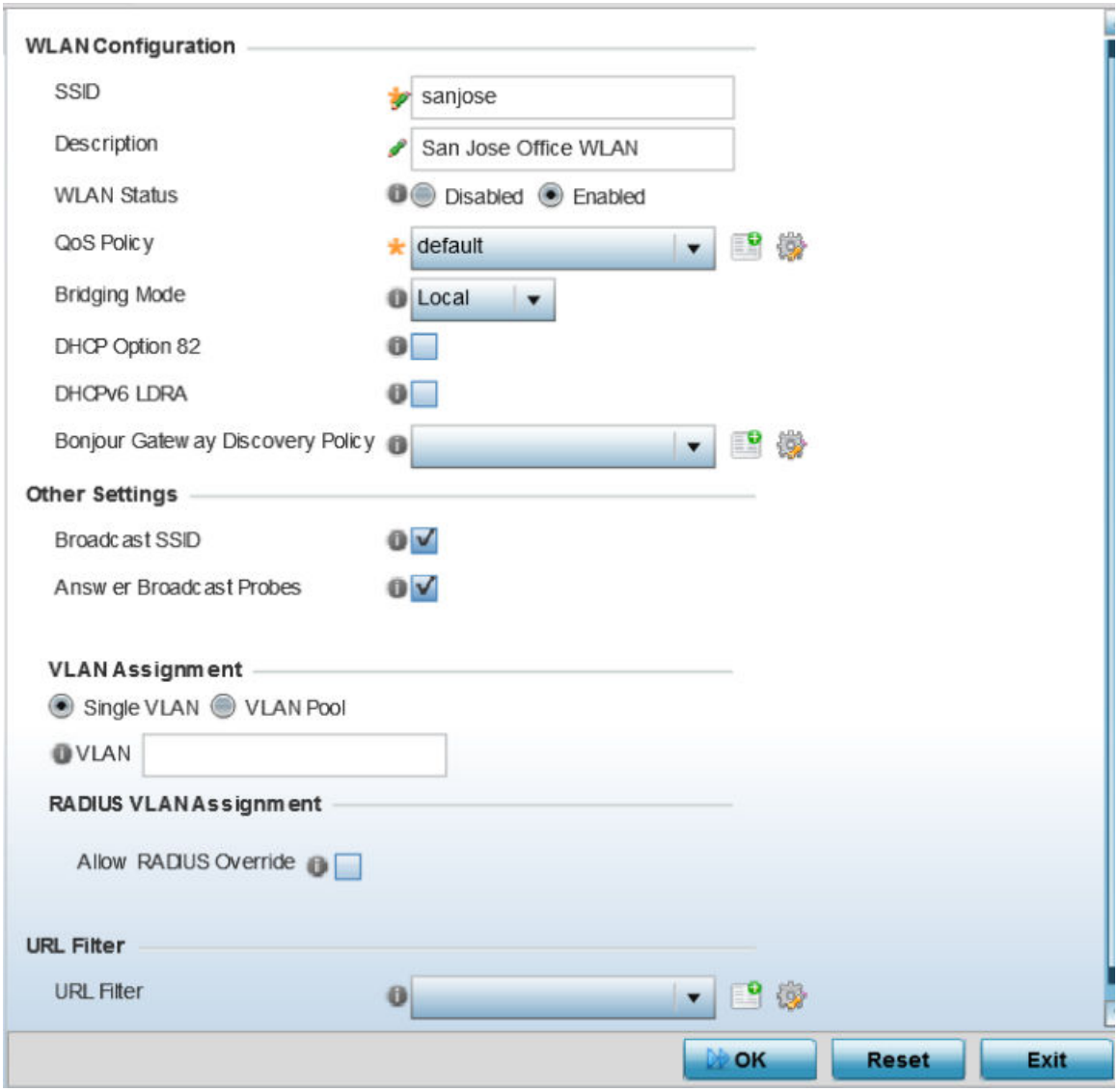



**Figure 272: WLAN Basic Configuration Screen**

3 Refer to the WLAN Configuration field to define the following:

| | |
|---|---|
| WLAN | If adding a new WLAN, enter its name in the space provided. Spaces between words or characters are not permitted. The name could be a logical representation of the WLAN support function (engineering, marketing etc.). If editing an existing WLAN, the WLAN's name appears at the top of the screen and cannot be modified. A WLAN name cannot exceed 32 characters. |
| SSID | Enter or modify the *Services Set Identification* (SSID) associated with the WLAN. The maximum number of characters that can be used for the SSID is 32. |
| Description | Provide a textual description for the WLAN to help differentiate it from others with similar configurations. The description can be up to 64 characters. |
| WLAN Status | Select the **Enabled** radio button to make this WLAN active and available to clients on all radios where it has been mapped. Select the **Disabled** radio button to make this WLAN inactive, meaning even if the WLAN is mapped to radios, it is not available for clients to associate and use. |

| | |
|---|---|
| QoS Policy | Use the drop-down menu to assign an existing QoS policy to the WLAN or select the **Create** icon to define a new QoS policy or select the **Edit** icon to modify the configuration of the selected QoS Policy. QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or per the proportion configured. For information on creating a QoS policy that can be applied to WLAN, see WLAN QoS Policies on page 604. |
| Bridging Mode | Use the drop-down menu to specify the WLAN's bridging mode as either **Local** or **Tunnel**. Select *Local* to bridge VLAN traffic locally, or *Tunnel* to use a shared tunnel for bridging the WLAN's VLAN traffic.<br><br>Note: The default setting is Local. |
| DHCP Option 82 | Select this option to enable DHCP option 82. DHCP Option 82 provides additional information about the physical attachment of a client.<br><br>Note: This setting is disabled by default. |
| DHCPv6 LDRA | Select this option to enable the DHCPv6 relay agent. The DHCPv6 LDRA allows for DHCPv6 messages to be transmitted on existing networks that do not currently support IPv6 or DHCPv6.<br><br>Note: This setting is disabled by default. |
| Bonjour Gateway Discovery Policy | Use the drop-down menu to assign an existing Bonjour Gateway Discovery policy to the WLAN. The Bonjour Gateway Discovery Policy configures how Bonjour services can be located on this WLAN. It configures the VLANs on which these services can be found. For more information on Bonjour Gateway Discovery Protocol, see Setting the Bonjour Gateway Configuration on page 814.<br>If needed, select the **Create** icon to define a new Bonjour Gateway Discovery policy or select the **Edit** icon to modify the configuration of a selected Bonjour Gateway Discovery Protocol. |

4 Refer to the Other Settings field to define broadcast behavior within this specific WLAN.

| | |
|---|---|
| Broadcast SSID | Select this check box to enable the broadcast of SSIDs within beacons. If a hacker tries to isolate and hack a SSID from a client, the SSID will display since the ESSID is in the beacon.<br><br>Note: This option is enabled by default. |
| Answer Broadcast Probes | Select this check box to associate a client with a blank SSID (regardless of which SSID the wireless controller is currently using).<br><br>Note: This option is enabled by default. |

5 Refer to the VLAN Assignment field to add or remove VLANs for the selected WLAN, and define the number of clients permitted. Remember, users belonging to separate VLANs can share the same WLAN. It's not necessary to create a new WLAN for every VLAN in the network.

| | |
|---|---|
| Single VLAN | Select this radio button to assign just one VLAN to this WLAN. If selecting this option, enter the name of the VLAN within the **VLAN** parameter field. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool. |
| VLAN Pool | Select this option to assign a set of VLANs to this WLAN. Use the table to configure the maximum number of clients that can use the configured per VLAN. Set a value in the range 0 - 8192 clients. |

6 Select **Allow Radius Override**, in the RADIUS VLAN Assignment field, to allow an override to the WLAN configuration. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in the RADIUS Access-Accept packet, and this feature is enabled, all client traffic is forward on that VLAN. If disabled, the RADIUS server returned VLAN-ID is ignored and the VLAN configuration (defined earlier) is used. In other words,

   If RADIUS authentication fails, the VLAN defined is the VLAN assigned to the WLAN.

7 Use the URL Filter field to configure user access restrictions to resources on the controller or service platform managed Internet. User access is controlled with URL Filters. Use the **URL Filter** drop down menu to select a preconfigured URL Filter. To create a new URL Filter, use the **Create** button. To edit an existing URL Filter, use the **Edit** button.

8 Select **OK** when completed to update the WLAN's basic configuration. Select **Reset** to revert the screen to the last saved configuration.

Before defining a WLAN's basic configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Deploy a separate VLAN for providing secure WLAN access.
- Define a separate VLAN for each WLAN providing guest access.

## Configuring WLAN Security

Assign WLANs unique security configurations supporting authentication, captive portal (hotspot), self registration or encryption schemes as data protection requirements dictate.

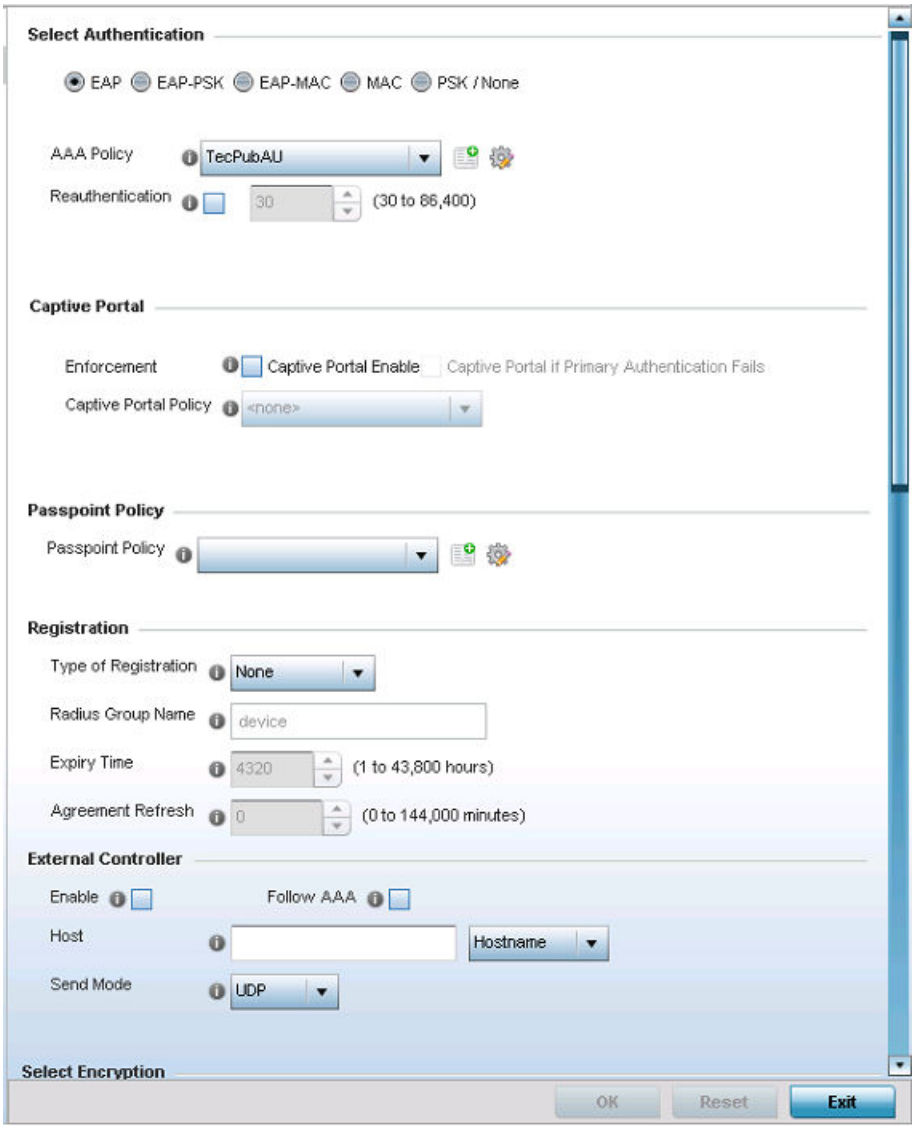



**Figure 273: WLAN Security Screen**

Authentication ensures that only known and trusted users or devices access a WLAN. Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information.

A client must authenticate to an access point to receive resources from the network. Controllers and service platforms support EAP, EAP PSK, EAP-MAC, MAC and PSK/None authentication options.

Refer to the following to configure an authentication scheme for a WLAN:

- 802.1x EAP, EAP-PSK and EAP MAC on page 558
- MAC Authentication on page 560
- PSK / None on page 561

Secure guest access to the network is referred to as captive portal access. A captive portal is guest access policy for providing guests temporary and restrictive access to the wireless network. Existing captive portal policies can be applied to a WLAN to provide secure guest access as needed.

A captive portal configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into captive portal, additional Agreement, Welcome and Fail pages provide the administrator with a number of options on captive portal screen flow and user appearance. Refer to Captive Portal on page 562 for information on assigning a captive portal policy to a WLAN.

A *passpoint* policy provides an interoperable platform for streamlining Wi-Fi access to access points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices. For more information, see Passpoint on page 562.

Encryption is central for WLAN security, as it provides data privacy for traffic forwarded over a WLAN. When the 802.11 specification was introduced, Wired Equivalent Privacy (WEP) was the primary encryption mechanism. WEP has since been interpreted as flawed in many ways, and is not considered an effective standalone encryption scheme for securing a wireless controller WLAN. WEP is typically used WLAN deployments designed to support legacy clients. New device deployments should use either WPA or WPA2 encryption.

Encryption applies a specific algorithm to alter its appearance and prevent unauthorized hacking. Decryption applies the algorithm in reverse, to restore the data to its original form. A sender and receiver must employ the same encryption/decryption method to interoperate. When both TKIP and CCMP are both enabled a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Since broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

TKIP-CCMP, WPA2-CCMP, WEP 64, WEP 128 and Keyguard encryption options are supported.

Refer to the following to configure an encryption scheme for a WLAN:

- TKIP-CCMP on page 564
- WPA2-CCMP on page 567
- WEP 64 on page 570
- WEP 128 on page 572
- Keyguard on page 574

### *802.1x EAP, EAP-PSK and EAP MAC*

The EAP *(Extensible Authentication Protocol)* is the de facto standard authentication method used to provide secure authenticated access to WLANs. EAP provides mutual authentication, secured credential exchange, dynamic keying and strong encryption. 802.1X EAP can be deployed with WEP, WPA or WPA2 encryption schemes to further protect user information forwarded over WLANs.

The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). An access point passes EAP packets from the client to an authentication server on the wired side of the access point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the client's identity.

802.1X EAP provides mutual authentication over the WLAN during authentication. The 802.1X EAP process uses credential verification to apply specific policies and restrictions to WLAN users to ensure access is only provided to specific wireless controller resources.

802.1X requires an 802.1X capable RADIUS server to authenticate users and a 802.1X client installed on each devices accessing the EAP supported WLAN. An 802.1X client is included with most commercial operating systems, including Microsoft Windows, Linux, and Apple OS X.

The RADIUS server authenticating 802.1X EAP users can reside either internally or externally to a controller, service platform or access point. User account creation and maintenance can be provided centrally using ADSP or individually maintained on each device. If an external RADIUS server is used, EAP authentication requests are forwarded.

When using PSK with EAP, the controller, service platform or access point sends a packet requesting a secure link using a pre-shared key. The authenticating device must use the same authenticating algorithm and passcode during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP. The only encryption types supported with this are TKIP, CCMP and TKIP-CCMP.

To configure EAP on a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
3 Select **Security**.
4 Select **EAP**, **EAP-PSK** or **EAP-MAC** as the **Authentication Type**.

   Each option enables the radio buttons for various encryption mechanisms as an additional measure of WLAN security.


**Figure 274: EAP, EAP-PSK or EAP MAC Authentication Screen**

5 Select an existing AAA Policy from the drop-down menu or select the **Create** icon to the right of the **AAA Policy** parameter to display a screen where new AAA policies can be created.

   Select the **Edit** icon to modify the configuration of the selected AAA policy.

   AAA *(authentication, authorization, and accounting)* is a framework for intelligently controlling access to the network, enforcing user authorization policies and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows.

   For information on defining a new AAA policy that can be applied to a WLAN supporting EAP, EAP PSK or EAP MAC, see AAA Policy.

6 Select the **Reauthentication** option to force EAP supported clients to reauthenticate.

Use the spinner control set the number of seconds (between 30 - 86,400) that, when exceeded, forces the EAP supported client to reauthenticate to use the WLAN.

7 Select **OK** when completed to update the WLAN's EAP configuration.

Select **Reset** to revert to the last saved configuration.

Before defining a 802.1x EAP, EAP-PSK or EAP MAC supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A valid certificate should be issued and installed on devices providing 802.1X EAP. The certificate should be issued from an Enterprise or public certificate authority to allow 802.1X clients to validate the identity of the authentication server prior to forwarding credentials.
- If using an external RADIUS server for EAP authentication, the round trip delay over the WAN should not exceed 150ms. Excessive delays over a WAN can cause authentication and roaming issues and impact wireless client performance. If experiencing excessive delays, consider using local RADIUS resources.

### *MAC Authentication*

MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP.

MAC authentication can be used for device level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static WEP, WPA-PSK and WPA2-PSK) MAC authentication can also be used to assign VLAN memberships, Firewall policies, and access restrictions based on time and date.

MAC authentication can only validate devices, not users. MAC authentication only references a client's wireless interface card MAC address when authenticating the device, it does not distinguish the device's user credentials. MAC authentication is somewhat poor as a standalone data protection technique, as MAC addresses can be easily spoofed by hackers who can provide a device MAC address to mimic a trusted device within the network.

MAC authentication is enabled per WLAN profile, augmented with the use of a RADIUS server to authenticate each device. A device's MAC address can be authenticated against the local RADIUS server built into the device or centrally (from a datacenter). For RADIUS server compatibility, the format of the MAC address can be forwarded to the RADIUS server in non-delimited and or delimited formats:

To configure MAC authentication on a WLAN:

1 Select **MAC** as the Authentication Type.

Selecting **MAC** enables the radio buttons for the Open, WEP 64, WEP 128, WPA/WPA2-TKIP, WPA2-CCMP and Keyguard encryption options as additional measures for the WLAN.


**Figure 275: MAC Authentication Screen**

2 Select an existing AAA Policy from the drop-down menu or select the **Create** icon to the right of the **AAA Policy** parameter to display a screen where new AAA policies can be created.

Select the **Edit** icon to modify the configuration of the selected AAA policy.

3 Select the **Reauthentication** option to force EAP supported clients to reauthenticate.

Use the spinner control set the number of seconds (between 30 - 86,400) that, when exceeded, forces the EAP supported client to reauthenticate to use the WLAN.

4 Select **OK** when completed to update the WLAN's MAC configuration.

Select **Reset** to revert to the last saved configuration.

*PSK / None*

Open-system authentication can be referred to as no authentication, since no actual authentication and user credential validation takes place. A client user requests (and is granted) authentication with no credential exchange.

Such a security-free convention may be appropriate in certain guest networks wherein no proprietary information purposely exposed to requesting clients, and their access to the controller, service platform or access point managed network is temporary and closely administrated.


**Figure 276: PSK / None Settings Screen**

Note

Although **None** implies no authentication, this option is also used when pre-shared keys are used for encryption (thus the PSK in the description).

*Captive Portal*

A *captive portal* is guest access policy for providing guests temporary and restrictive access to the network. The primary means of securing such guest access is the use of a captive portal. For an overview of the captive portal process and information on how to define a captive portal policy, see Captive Portal Policies on page 785.

To assign a captive portal policy to a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
3 Select **Security**.
4 Refer to the **Captive Portal** section in the WLAN Policy security screen.

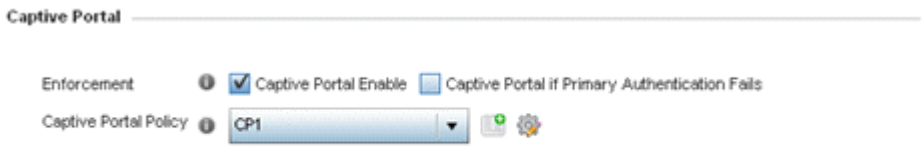



**Figure 277: WLAN Policy Security Screen - Captive Portal Field**

5 Select **Captive Portal Enable** if authenticated guest access is required with the selected WLAN.

This feature is disabled by default.

6 Select **Captive Portal if Primary Authentication Fails** to enable the captive portal policy if the primary authentication is unavailable.

This option is enabled only when **Captive Portal Enable** is selected.

7 Select the **Captive Portal Policy** to use with the WLAN from the drop-down menu.

If no relevant policies exist, select the **Create** icon to define a new policy to use with this WLAN or the **Edit** icon to update the configuration of an existing Captive Portal policy. For more information, see Captive Portal Policies on page 785.

8 Select **OK** when completed to update the WLAN's captive portal configuration.

Select **Reset** to revert to the last saved configuration.

*Passpoint*

A *passpoint policy* provides an interoperable platform for streamlining Wi-Fi access to access points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices.

To assign a passpoint policy to a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
3 Select **Security**.

4 Refer to the **Passpoint** field in the WLAN Policy security screen.


**Figure 278: WLAN Policy Security Screen - Passpoint Policy**

5 Select an existing passpoint policy from the drop down menu to apply it to the WLAN.

If no relevant policies exist, select the **Create** icon to define a new policy to use with this WLAN or the **Edit** icon to update the configuration of an existing passpoint policy. For more information on Passpoint Policy, see Passpoint Policy on page 660.

6 Select **OK** when completed to update the WLAN's passpoint policy configuration.

Select **Reset** to revert to the last saved configuration.

*MAC Registration*

MAC Registration provides returning (previously validated) clients quick access to controller, service platform or access point managed captive portal resources.

When a user enters a captive portal for the first time, user data is gathered and stored. This information is matched against the MAC address of the device accessing the captive portal.

The next time a user accesses the captive portal using this same credentials, they are authenticated immediately, since the device's MAC address is available within the controller, service platform or access point's database along with the requester's identification information. There's no need for additional credential validation after the initial credential verification.

To assign MAC Registration to a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.

2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.

3 Select **Security**.

4 Refer to the **Registration** field in the WLAN security screen.

Select the **Type of Registration** field to select the type of MAC registration to use with this WLAN.

Use **None** to disallow use of MAC Registration with this WLAN. Select device to register a new MAC address. If a MAC address already exists, allow access. Select **device-OTP** to register a new MAC device and send a OTP *(One Time Password)* for validation. Select user to register a new user by sending them a registration code to the e-mail address or mobile phone number provided by the user at login.

5 Use the **RADIUS Group Name** field to enter the RADIUS group to associate with MAC registrations.

When left blank, devices are not associated with a RADIUS group.

6 Select **Expiry Time**.

This is the duration for which MAC addresses are stored on the access point's database. Once this time expires, the user information is purged from the database. The user then has to provide login credentials as well as identification information again. The default value is 1500 days.

7 Set the **Agreement Refresh** as the amount of time before the agreement page is displayed if the user has not been logged during the specified period.

The default setting is 0 days.

8 Select **OK** when completed to update the WLAN's MAC registration configuration.

Select **Reset** to revert to the last saved configuration.

*External Controller*

An external configuration enables a WLAN to be managed remotely from either a controller or access point. However, this feature is disabled by default and must be manually enabled.

To set a WLAN's external security configuration:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.

2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.

3 Select **Security**.

4 Refer to the **External Controller** section in the WLAN Policy security screen.


**Figure 279: WLAN Policy Security Screen - External Controller Field**

5 Select the **Enable** option if WLAN authentication is to be handled using an external resource.

6 Use the **Host** field to enter a hostnameor IP address of the remote wireless controller.

Use the spinner control to select the type of the remote controller.

7 Use the **Proxy Mode** drop-down to configure the proxy mode for accessing remote resources.

8 Select **OK** when completed to update the WLAN's external controller configuration.

Select **Reset** to revert to the last saved configuration.

*TKIP-CCMP*

WPA *(Wi-Fi Protected Access)* is an encryption scheme specified in the IEEE *Wireless Fidelity* standard 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

The encryption method is TKIP *(Temporal Key Integrity Protocol)*. TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check and an extended initialization vector. However, TKIP also has vulnerabilities.

CCMP is a security standard used by the AES *(Advanced Encryption Standard)*. AES serves the same function TKIP does for WPA-TKIP. CCMP computes a MIC *(Message Integrity Check)* using the proven

CBC *(Cipher Block Chaining)* technique. Changing just one bit in a message produces a totally different result.

To configure TKIP-CCMP encryption on a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.

2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.

3 Select **Security**.

4 Select the **TKIP-CCMP** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a TKIP-CCMP configuration for the WLAN.

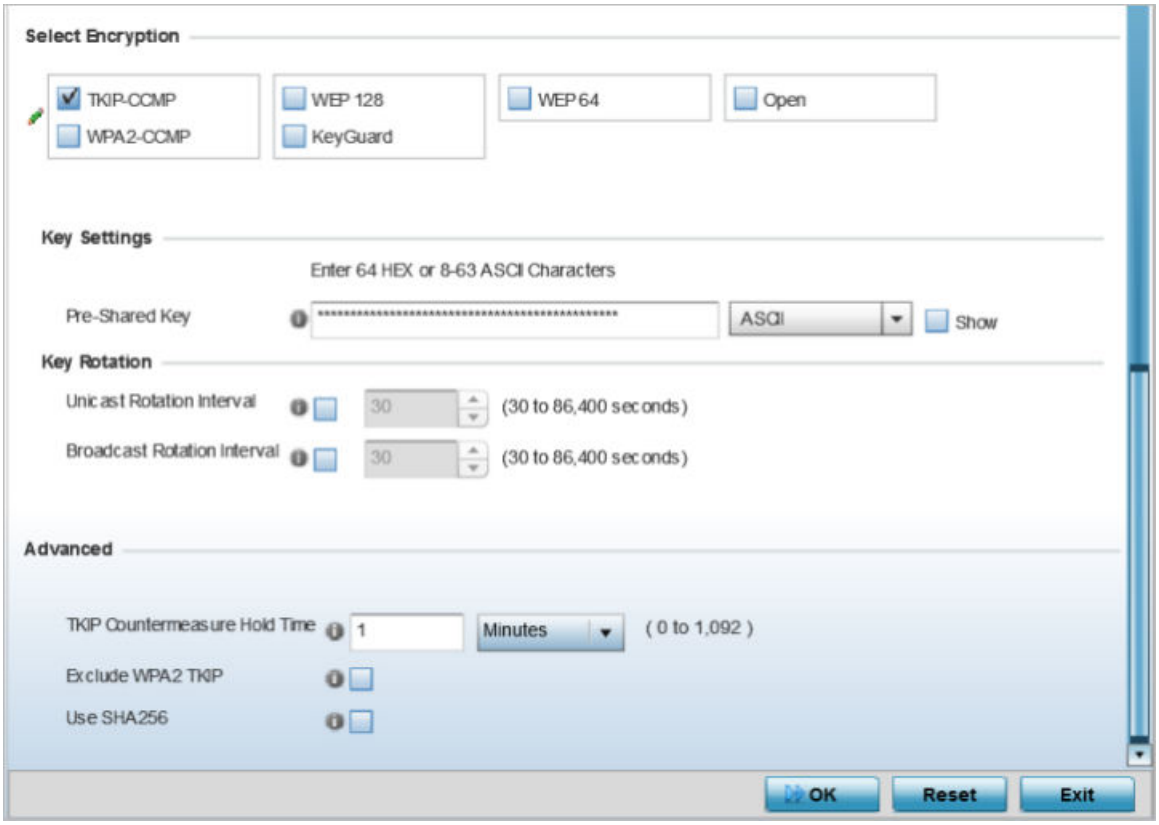



**Figure 280: WLAN Security - TKIP-CCMP Screen**

5 Define **Key Settings**.

| | |
|---|---|
| Pre-Shared Key | Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converetd to to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated. |

6 Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. Broadcast messages are addressed to multiple devices. When using WPA2, a wireless client can use two keys: one unicast key, for its own traffic to and from an access point, and one broadcast key, the common key for all the clients in that subnet.

Rotating the keys is recommended the keys so a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

| | |
|---|---|
| Unicast Rotation Interval | Define an interval for unicast key transmission interval from 30 - 86,400 seconds. Some clients have issues using unicast key rotation, so ensure you know which kind of clients are impacted before using unicast keys. This feature is disabled by default. |
| Broadcast Rotation Interval | When enabled, the key indices used for encrypting and decrypting broadcast traffic is alternatively rotated based on the defined interval. Define a broadcast key transmission interval from 30 - 86,400 seconds. Key rotation enhances the broadcast traffic security on the WLAN. This feature is disabled by default. |

7 Define the **Fast Roaming** configuration used only with 802.1x EAP-WPA/WPA2 authentication.

Note

Fast Roaming is available only when the authentication is **EAP** or **EAP-PSK** and the selected encryption is either **TKIP-CCMP** or **WPA2-CCMP**.

Using 802.11i can speed up the roaming process from one access point to another. Instead of doing a complete 802.1x authentication each time a client roams between access points, 802.11i allows a client to re-use previous PMK authentication credentials and perform a four-way handshake. This speeds up the roaming process. In addition to reusing PMKs on previously visited access points, **Opportunistic Key Caching** allows multiple access points to share PMKs among themselves. This allows a client to roam to an access point it has not previously visited and reuse a PMK from another access point to skip 802.1x authentication.

| | |
|---|---|
| Pre-Authentication | Selecting this option enables an associated client to carry out an 802.1x authentication with another access point before it roams to it. This enables a roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. With pre-authentication, a client can perform an 802.1X authentication with other detected access points while still connected to its current access point. When a device roams to a neighboring access point, the device is already authenticated on the access point, thus providing faster re-association. |
| Pairwise Master Key (PMK) Caching | *Pairwise Master Key* (PMK) caching is a technique for sidestepping the need to re-establish security each time a client roams to a different switch. Using PMK caching, clients and switches cache the results of 802.1X authentications. Therefore, access is much faster when a client roams back to a switch to which the client is already authenticated. |
| Opportunistic Key Caching | This option enables the access point to use a PMK derived with a client on one access point, with the same client when it roams over to another access point. Upon roaming, the client does not have to do 802.1x authentication and can start sending and receiving data sooner. |

8 Set the following **Advanced** settings for the TKIP-CCMP encryption scheme:

| | |
|---|---|
| TKIP Countermeasure Hold Time | The **TKIP Countermeasure Hold Time** is the time a WLAN is disabled, if TKIP countermeasures have been invoked on the WLAN. Use the drop-down menu to define a value in either Hours (0-18), Minutes (0-1,092) or Seconds (0-65,535). The default setting is 1 second. |
| Exclude WPA2-TKIP | Select this option to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP, but do not support WPA2-CCMP. We recommend that you enable this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2- CCMP enabled clients. This feature is disabled by default. |
| Use SHA256 | Select this option to enable SHA-256 authentication key management suite. This suite consists of a set of algorithms for key agreement, key derivation, key wrapping, and content encryption and provide a minimum cryptographic security level of 128 bits. This feature is disabled by default. |

9 Select **OK** when completed to update the WLAN's TKIP-CCMP encryption configuration.

Select **Reset** to revert to the last saved configuration.

Before defining a WPA-TKIP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Enable TKIP for legacy device support only when WPA2-CCMP support is not available.
- Although TKIP offers better security than WEP, it can be vulnerable to certain attacks.
- When both TKIP and CCMP are enabled, a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Because broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

*WPA2-CCMP*

WPA2 is a newer 802.11i standard that provides even stronger wireless security than WPA *(Wi-Fi Protected Access)* and WEP. CCMP is the security standard used by the AES *(Advanced Encryption Standard )*. AES serves the same function TKIP does for WPA-TKIP. CCMP computes a MIC *(Message Integrity Check)* using the proven CBC *(Cipher Block Chaining)* technique. Changing just one bit in a message produces a totally different result.

WPA2/CCMP is based on the concept of a RSN *(Robust Security Network)*, which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any a controller, service platform or Access Point provides for its connected clients.

To configure WPA2-CCMP encryption on a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
3 Select **Security**.

4 Select the **WPA2-CCMP** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a WPA2-CCMP configuration for the new or existing WLAN.

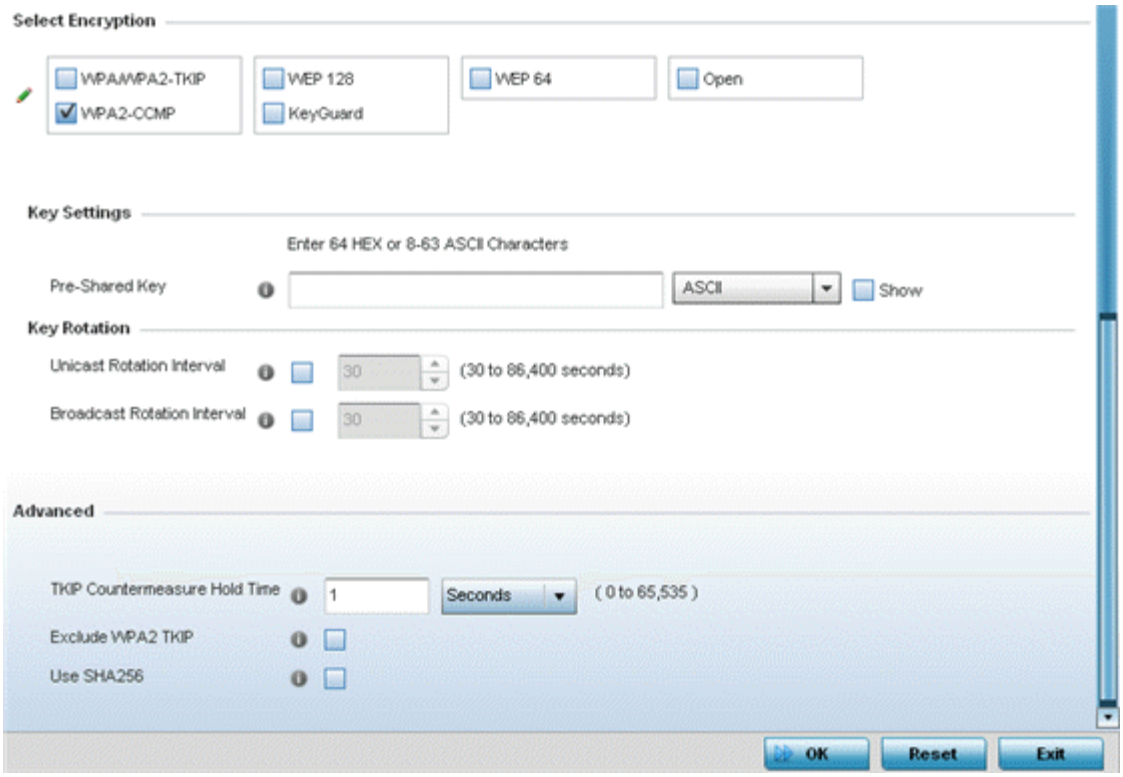



**Figure 281: WLAN Security - WPA2-CCMP Screen**

5 Define **Key Settings**.

| | |
|---|---|
| Pre-Shared Key | Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converetd to to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated. |

6 Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. Broadcast messages are addressed to multiple devices. When using WPA2, a wireless client can use two keys: one unicast key, for its own traffic to and from an Access Point, and one broadcast key, the common key for all the clients in that subnet.

Rotating the keys is recommended the keys so a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

| | |
|---|---|
| Unicast Rotation Interval | Define an interval for unicast key transmission interval from 30 - 86,400 seconds. Some clients have issues using unicast key rotation, so ensure you know which kind of clients are impacted before using unicast keys. This feature is disabled by default. |
| Broadcast Rotation Interval | When enabled, the key indices used for encrypting and decrypting broadcast traffic is alternatively rotated based on the defined interval. Define a broadcast key transmission interval from 30 - 86,400 seconds. Key rotation enhances the broadcast traffic security on the WLAN. This feature is disabled by default. |

7 Define the **Fast Roaming** configuration used only with 802.1x EAP-WPA/WPA2 authentication.

Note

Fast Roaming is available only when the authentication is **`EAP`** or **`EAP-PSK`** and the selected encryption is either **`TKIP-CCMP`** or **`WPA2-CCMP`**.

Using 802.11i can speed up the roaming process from one access point to another. Instead of doing a complete 802.1x authentication each time a client roams between access points, 802.11i allows a client to re-use previous PMK authentication credentials and perform a four-way handshake. This speeds up the roaming process. In addition to reusing PMKs on previously visited access points, **Opportunistic Key Caching** allows multiple access points to share PMKs among themselves. This allows a client to roam to an access point it has not previously visited and reuse a PMK from another access point to skip 802.1x authentication.

| | |
|---|---|
| Pre-Authentication | Selecting this option enables an associated client to carry out an 802.1x authentication with another access point before it roams to it. This enables a roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. With pre-authentication, a client can perform an 802.1X authentication with other detected access points while still connected to its current access point. When a device roams to a neighboring access point, the device is already authenticated on the access point, thus providing faster re-association. |
| Pairwise Master Key (PMK) Caching | *Pairwise Master Key* (PMK) caching is a technique for sidestepping the need to re-establish security each time a client roams to a different switch. Using PMK caching, clients and switches cache the results of 802.1X authentications. Therefore, access is much faster when a client roams back to a switch to which the client is already authenticated. |
| Opportunistic Key Caching | This option enables the access point to use a PMK derived with a client on one access point, with the same client when it roams over to another access point. Upon roaming, the client does not have to do 802.1x authentication and can start sending and receiving data sooner. |

8 Set the following **Advanced** settings for the WPA2-CCMP encryption scheme:

| | |
|---|---|
| TKIP Countermeasure Hold Time | The **TKIP Countermeasure Hold Time** is the time a WLAN is disabled, if TKIP countermeasures have been invoked on the WLAN. Use the drop-down menu to define a value in either Hours (0-18), Minutes (0-1,092) or Seconds (0-65,535). The default setting is 1 second. |
| Exclude WPA2-TKIP | Select this option to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP, but do not support WPA2-CCMP. We recommend that you enable this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2- CCMP enabled clients. This feature is disabled by default. |
| Use SHA256 | Select this option to enable SHA-256 authentication key management suite. This suite consists of a set of algorithms for key agreement, key derivation, key wrapping, and content encryption and provide a minimum cryptographic security level of 128 bits. This feature is disabled by default. |

9 Select **OK** when completed to update the WLAN's WPA2-CCMP encryption configuration.

Select **Reset** to revert to the last saved configuration.

Before defining a WPA2-TKIP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WPA2-CCMP should be configured for all new (non-visitor) WLANs requiring encryption, as it's supported by the majority of the hardware and client vendors using wireless networking equipment.
- WPA2-CCMP supersedes WPA-TKIP and implements all the mandatory elements of the 802.11i standard. WPA2- CCMP introduces a new AES-based algorithm called CCMP which replaces TKIP and WEP and is considered significantly more secure.

*WEP 64*

WEP *(Wired Equivalent Privacy)* is a security protocol specified in the IEEE Wi-Fi *(Wireless Fidelity)* standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP can be used with open, shared, MAC and 802.1 X EAP authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered. If 802.1X support is not available on the legacy device, MAC authentication should be enabled to provide device level authentication.

WEP 64 uses a 40-bit key concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP 64 is a less robust encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw. WEP is only recommended when clients are incapable of using more robust forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP 64 encryption on a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.

2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.

3 Select **Security**.

4 Select the **WEP 64** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a WEP 64 configuration for the new or existing WLAN.

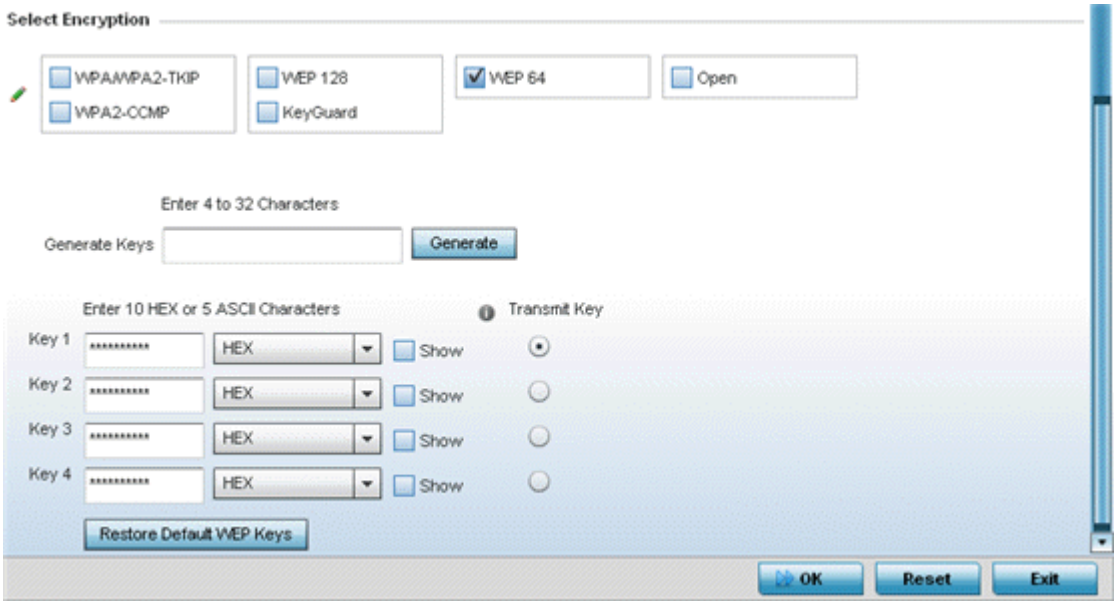



**Figure 282: WLAN Security - WEP 64 Screen**

5 Configure the following WEP 64 settings:

| | |
|---|---|
| Generate Keys | Specify a 4- to 32-character pass key and click **Generate**. The pass key can be any alphanumeric string. The controller or Access Point and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. |
| Keys 1-4 | Use the **Key #1-4** fields to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting **Show** displays a key in exposed plain text. |
| Restore Default WEP Keys | Select this button to restore the WEP algorithm to its default settings. |

Default WEP 64 keys are as follows:

- Key 1 1011121314
- Key 2 2021222324
- Key 3 3031323334
- Key 4 4041424344

6 Select **OK** when completed to update the WLAN's WEP 64 encryption configuration.

Select **Reset** to revert to the last saved configuration.

Before defining a WEP 64 supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Additional layers of security (beyond WEP) should be enabled to minimize the likelihood of data loss and security breaches. WEP enabled WLANs should be mapped to an isolated VLAN with firewall policies restricting access to hosts and suspicious network applications.

- WEP enabled WLANs should be permitted access only to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should also be configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

*WEP 128*

WEP *(Wired Equivalent Privacy)* is a security protocol specified in the IEEE Wi-Fi *(Wireless Fidelity)* standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP can be used with open, shared, MAC and 802.1 X EAP authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered. If 802.1X support is not available on the legacy device, MAC authentication should be enabled to provide device level authentication.

WEP 128 and Keyguard use a 104-bit key which is concatenated with a 24-bit IV *(initialization vector)* to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. WEP is recommended only when there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

WEP 128 or Keyguard provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys.

To configure WEP 128 encryption on a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
3 Select **Security**.

4 Select the **WEP 128** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a WEP 128 configuration for the new or existing WLAN.

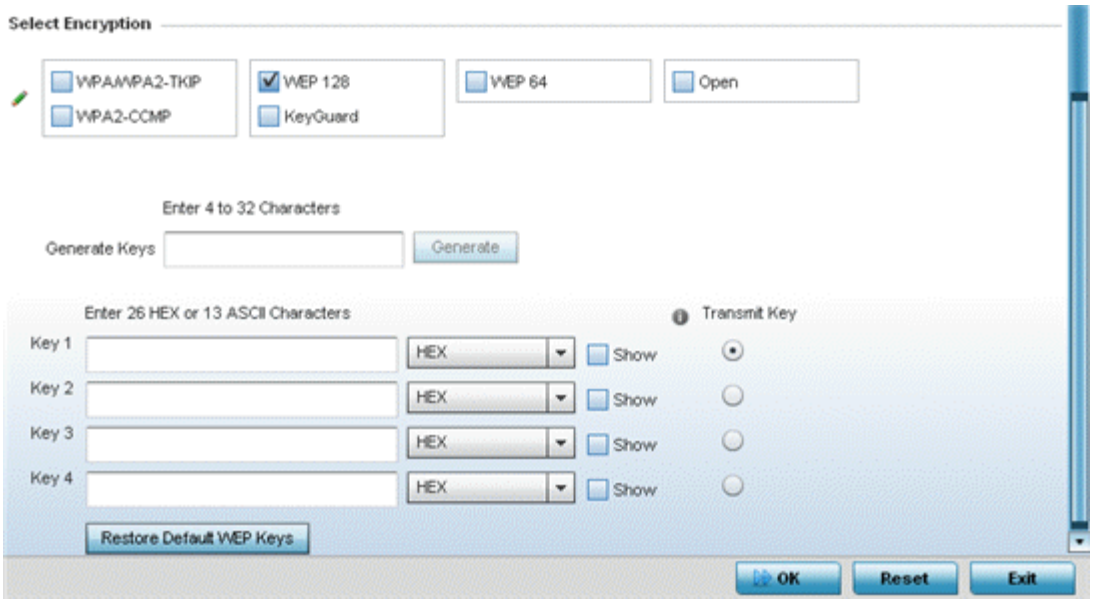



**Figure 283: WLAN Security - WEP 128 Screen**

5 Configure the following WEP 128 settings:

| | |
|---|---|
| Generate Keys | Specify a 4- to 32-character pass key and click **Generate**. TThe pass key can be any alphanumeric string. The access point, other proprietary routers, and WiNG clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without these WiNG adapters need to use WEP keys manually configured as hexadecimal numbers. |
| Keys 1-4 | Use the **Key #1-4** fields to specify key numbers. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting **Show** displays a key in exposed plain text. |
| Restore Default WEP Keys | Select this button to restore the WEP algorithm to its default settings. |

Default WEP 128 keys are as follows:

- Key 1 10111213141516171819 1A1B1C
- Key 2 20212223242526272829 2A2B2C
- Key 3 30313233343536373839 3A3B3C
- Key 4 40414243444546474849 4A4B4C

6 Select **OK** when completed to update the WLAN's WEP 128 encryption configuration.

Select **Reset** to revert to the last saved configuration.

Before defining a WEP 128 supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Additional layers of security (beyond WEP) should be enabled to minimize the likelihood of data loss and security breaches. WEP enabled WLANs should be mapped to an isolated VLAN with firewall policies restricting access to hosts and suspicious network applications.

- WEP enabled WLANs should be permitted access only to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should also be configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

*Keyguard*

Keyguard (a form of WEP) could be all a small business needs for the simple encryption of wireless data.

Keyguard is a proprietary encryption method and an enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. The Keyguard encryption implementation is based on the IEEE Wi-Fi standard, 802.11i.

To configure Keyguard encryption on a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
3 Select **Security**.
4 Select the **Keyguard** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a keyguard configuration for the new or existing WLAN.

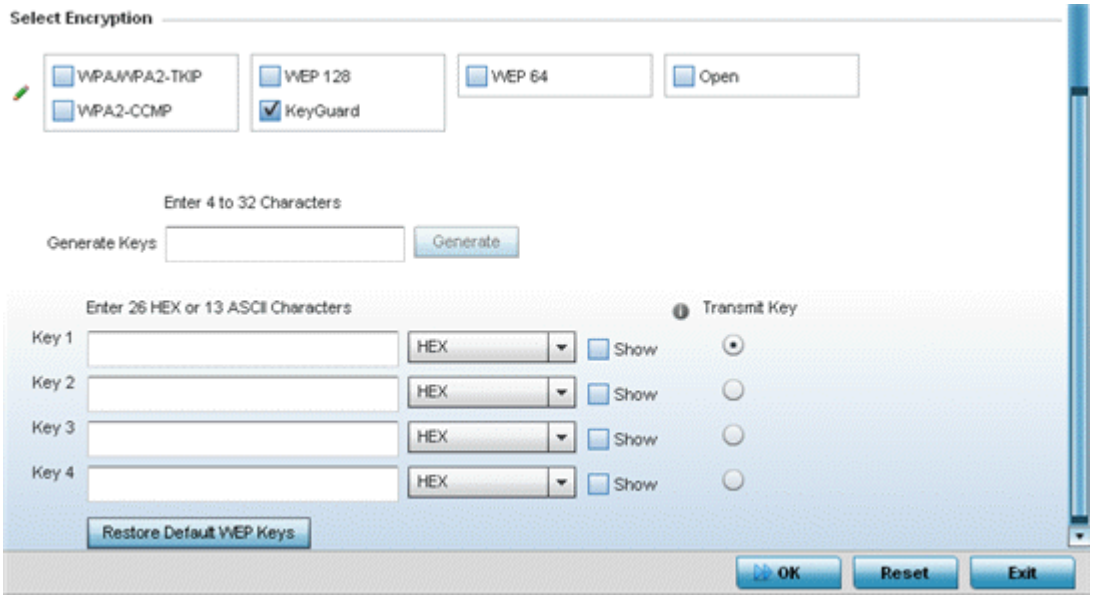



**Figure 284: WLAN Security - Keyguard Screen**

5 Configure the following keyguard settings:

| | |
|---|---|
| Generate Keys | Specify a 4- to 32-character pass key and click **Generate**. TThe pass key can be any alphanumeric string. The access point, other proprietary routers, and WiNG clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without these WiNG adapters need to use keys manually configured as hexadecimal numbers. |
| Keys 1-4 | Use the **Key #1-4** fields to specify key numbers. For keyguard (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting **Show** displays a key in exposed plain text. |
| Restore Default WEP Keys | Select this button to restore the keyguard algorithm to its default settings. This might be necessary, for example, if the latest defined algorithm has been compromised and no longer provides its former measure of data security. |

Default WEP keyguard keys are as follows:

- Key 1 101112131415161718191A1B1C
- Key 2 202122232425262728292A2B2C
- Key 3 303132333435363738393A3B3C
- Key 4 404142434445464748494A4B4C

6 Select **OK** when completed to update the WLAN's keyguard encryption configuration.

Select **Reset** to revert to the last saved configuration.

Before defining a keyguard configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WiNG proprietary authentication techniques can also be enabled on WLANs supporting other WiNG proprietary techniques, such as keyguard.
- A WLAN using keyguard to support legacy devices should largely limit its use of keyguard to those legacy devices only.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should be also configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

## Configuring WLAN Firewall Settings

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a Firewall can be thought of as mechanisms *allowing* and *denying* data traffic in respect to administrator defined rules. For an overview of Firewalls, see Wireless Firewall on page 730.

WLANs use Firewalls like ACLs *(Access Control Lists)* to filter/mark packets based on the WLAN from which they arrive, as opposed to filtering packets on Layer 2 ports. An ACL contains an ordered list of ACEs *(Access Control Entries)*. Each ACE specifies an action and a set of conditions (rules) a packet must satisfy to match the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP based Firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC Firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical *allow*, *deny* or *mark* designation to WLAN packet traffic.

A MAC Firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to WLAN packet traffic.

Keep in mind that IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

To review existing Firewall configurations, create a new Firewall configuration or edit the properties of a WLAN's existing Firewall:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify the properties of an existing WLAN.
3 Select **Firewall** from the Wireless LAN Policy options.

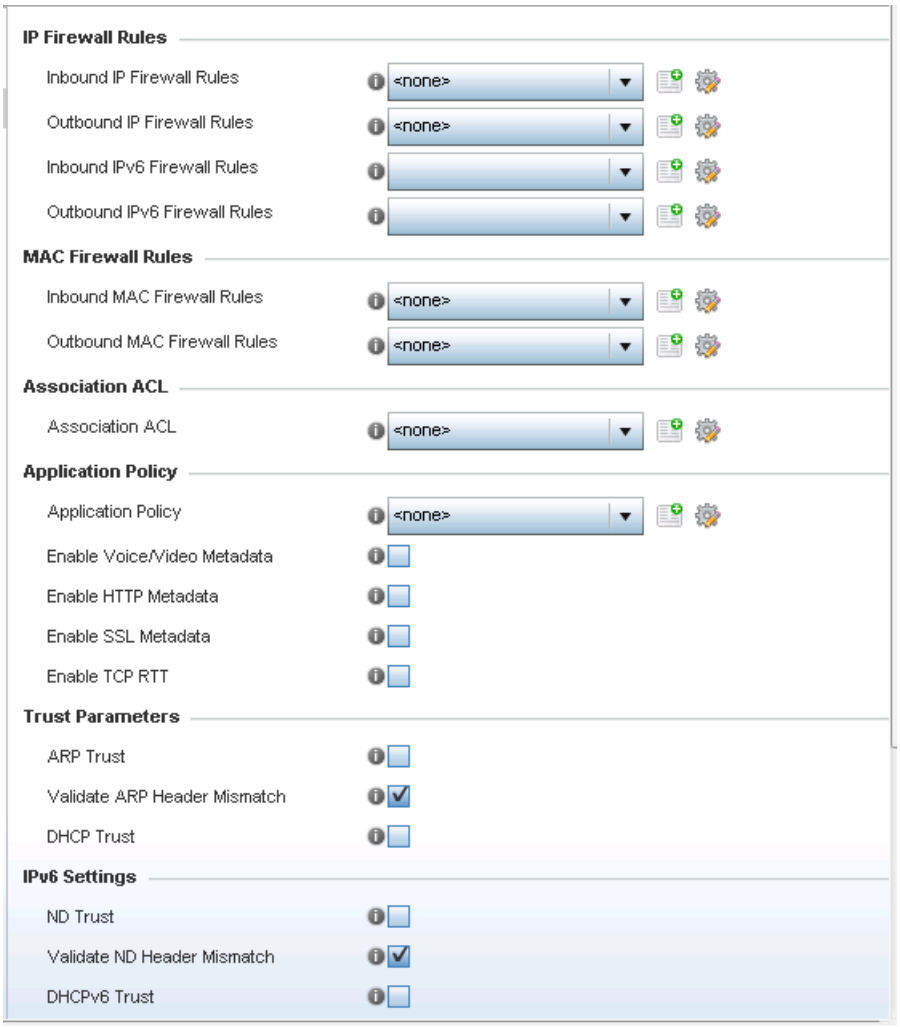



**Figure 285: WLAN Security - WLAN Firewall Screen**

4 Select one of the following, using the drop-down menu:

- Inbound IP Firewall Rule
- Outbound IP Firewall Rule
- Inbound IPv6 Firewall Rules
- Outbound IPv6 Firewall Rule

If no rules exist, select the **Create** icon to create a new firewall rule configuration. Select the **Edit** icon to modify the configuration of a selected Firewall policy configuration.

If you are creating a new rule, provide a name up to 32 characters.

5 Click **Add**.

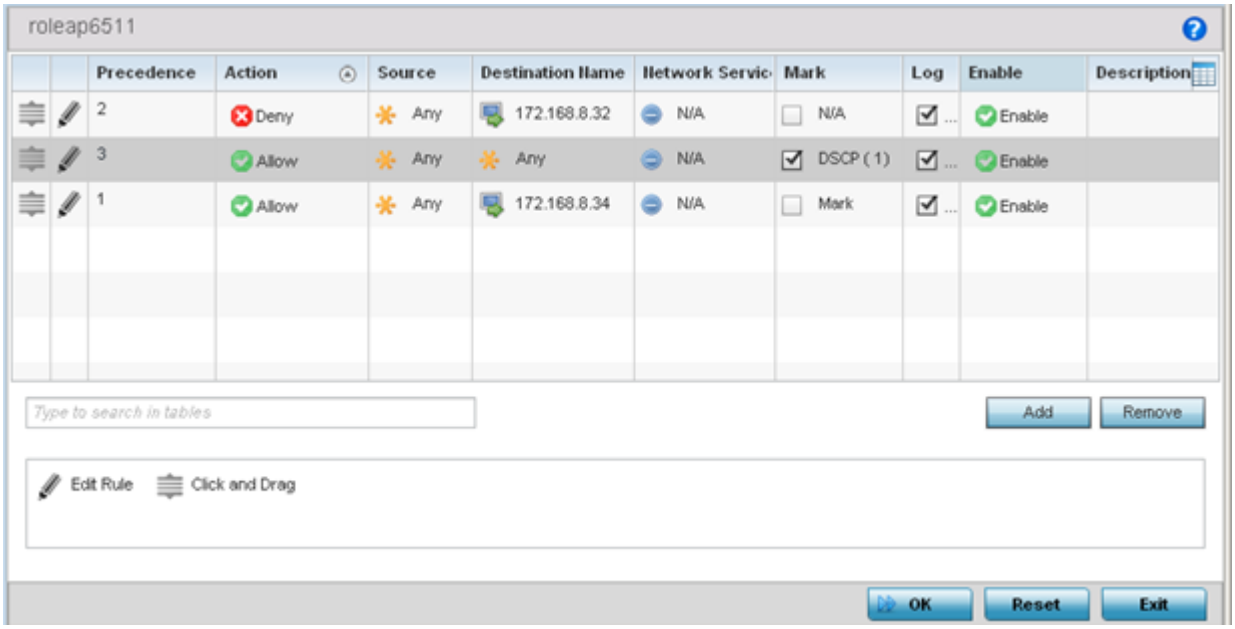



**Figure 286: WLAN Security - IP Firewall Rules Screen**

6 IP firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

a Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.

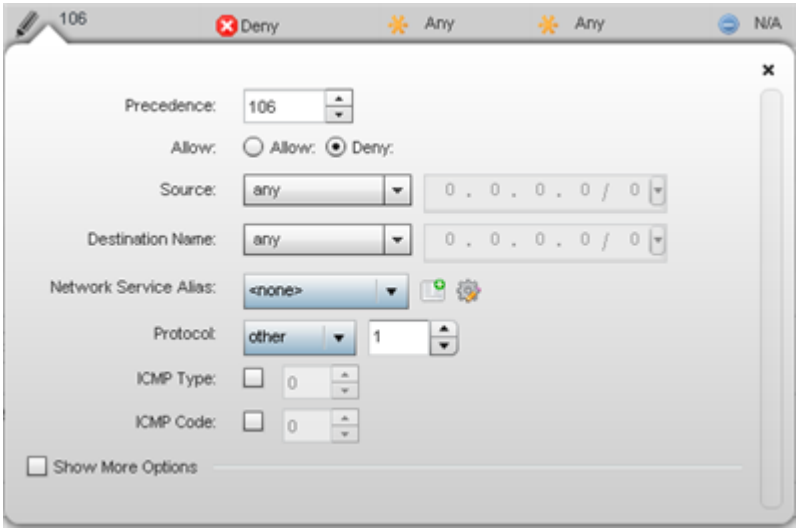



**Figure 287: WLAN Security - IP Firewall Rules - Edit Rule Screen**

b Click the icon in the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.


**Figure 288: WLAN Security - IP Firewall Rules - IP Firewall Rules Add Criteria**

Note

Only those selected IP ACL filter attributes display. Each value can have its current setting adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

7 Define the following parameters for either inbound or outbound IP firewall rules:

| | |
|---|---|
| Precedence | Specify or modify a precedence for this IP policy between 1 and 5000. Rules with lower precedence are always applied to packets first. If you modify a precedence to apply a higher integer, it will move down the table to reflect its lower priority. |
| Action | Every IP Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:<br>**Deny** Instructs the Firewall to prohibit a packet from proceeding to its destination<br>**Allow** Instructs the Firewall to allow a packet to proceed to its destination |
| DNS Name | Specify the DNS Name which may be a full domain name, a portion of a domain name or a suffix. This name is used for the **DNS Match Type** criteria. |
| DNS Match Type | Specify the DNS matching criteria that the DNS Name can be matched against. This can be configured as an exact match for a DNS domain name, a suffix for the DNS name or a domain that contains a portion of the DNS name. If traffic matches the configured criteria in the DNS Match Type, that rule will be applied to the ACL. |
| Source | Select the source IP address or network group configuration used as basic matching criteria for this IP ACL rule. Source options include:<br>• Any – Indicates any host device in any network.<br>• Network – Indicates all hosts in a particular network. Subnet mask information must be provided for filtering based on network.<br>• Host – Indicates a single host with a specific IP address.<br>• Alias – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL. |
| Destination | Select the destination IP address or network group configuration used as a basis matching criteria for this IP ACL rule. Destination options include:<br>• Any – Indicates any host device in any network.<br>• Network – Indicates all hosts in a particular network. Subnet mask information must be provided for filtering based on network.<br>• Host – Indicates a single host with a specific IP address.<br>• Alias – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of ACL configuration. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL. |
| Protocol | Select the protocol to filter for this ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number. |
| Network Service Alias | The *service alias* is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant. Selecting either **tcp** or **udp** displays an additional set of specific TCP/UDP source and destination port options. |

| | |
|---|---|
| Source Port | If you are using either **tcp** or **udp** as the protocol, define whether the source port for incoming IP ACL rule application is **any**, **equals**, or an administrator defined range. If you are not using **tcp** or **udp**, this setting displays as N/A. This is the data local origination port designated by the administrator. Selecting **equals** invokes a spinner control for setting a single numeric port.<br>Selecting **equals** invokes a spinner control for setting a single numeric port.<br>Selecting **range** displays spinner controls for low and high numeric range settings.<br>A source port cannot be a destination port. |
| Destination Port | If you are using either **tcp** or **udp** as the protocol, define whether the destination port for outgoing IP ACL rule application is **any**, **equals**, or an administrator defined range. If you are not using **tcp** or **udp**, this setting displays as N/A. This is the data destination virtual port designated by the administrator.<br>Selecting **equals** invokes a spinner control for setting a single numeric port.<br>Selecting **range** displays spinner controls for low and high numeric range settings.<br>A source port cannot be a destination port. |
| ICMP Type | Selecting **ICMP** as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The ICMP *(Internet Control Message Protocol)* uses messages identified by numeric type. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10. |
| ICMP Code | Selecting **ICMP** as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding code, helpful for troubleshooting network issues, for example *0 - Net Unreachable*, *1 - Host Unreachable*, and *2 - Protocol Unreachable*. |
| Start VLAN | Select a **Start VLAN** icon within a table row to set (apply) a start VLAN range for this IP ACL filter. The Start VLAN represents the virtual LAN beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply. |
| End VLAN | Select an **End VLAN** icon within a table row to set (apply) an end VLAN range for this IP ACL filter. The End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply. |
| Mark | Select this option to mark certain fields inside a packet before allowing them. Mark applies only for **Allow** rules. Mark sets the rule's 802.1p or dscp level (from 0 - 7) |
| Log | Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed. |
| Enabled | Select this option to enable or disable this particular IP Firewall rule in this rule set. |
| Description | Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a Select Columns screen used to add or remove IP ACL criteria from the table. |

8 The **Precedence** column sets the priority of a IP Firewall rule within its rule set.

Click on this column and drag the rule to its appropriate place in the ruleset to set its precedence.

9 Select an existing Inbound IPv6 Firewall Rule or Outbound IPv6 Firewall Rule using the drop-down menu.

If no rules exist, select the **Create** icon to create a new firewall rule configuration. Select the Edit icon to modify the configuration of a selected firewall.

If creating a new rule, provide a name up to 32 characters.

10 Click **Add**.

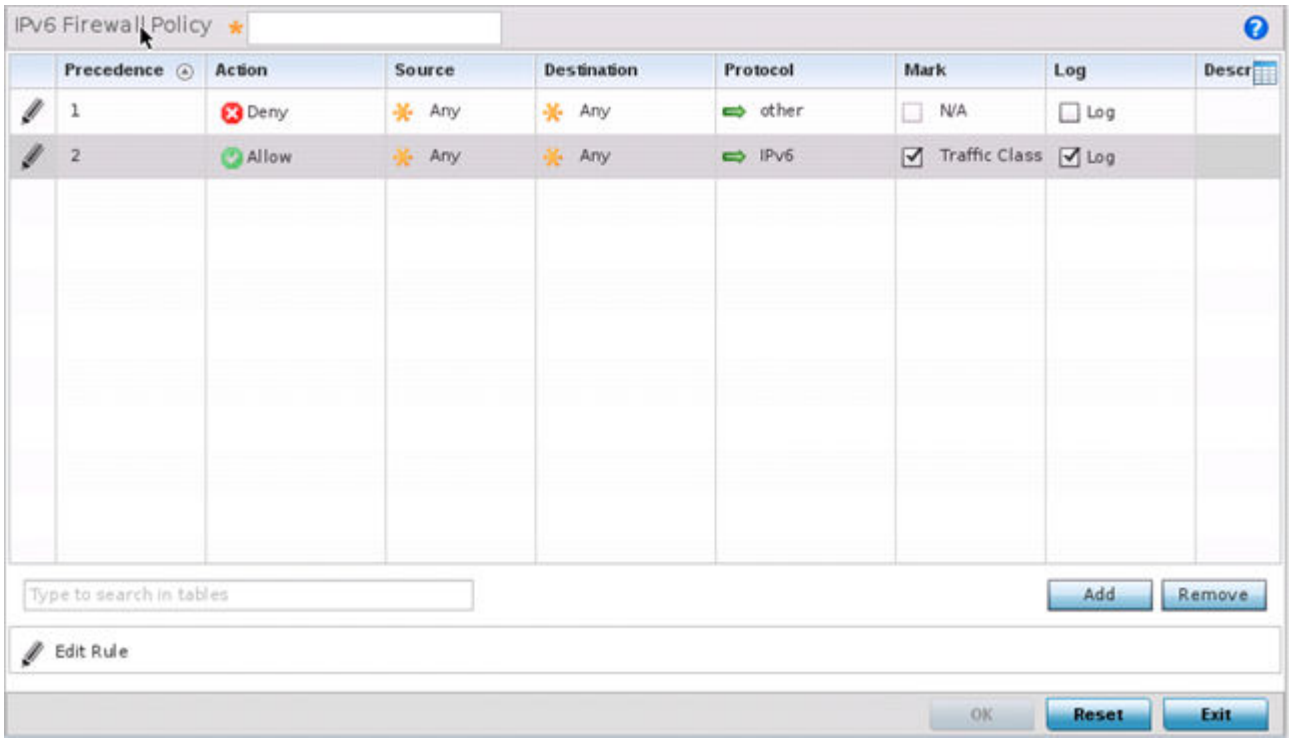



**Figure 289: WLAN Security - IPv6 Firewall Rules screen**

IPv6 Firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

11 Select the **Edit Rule** icon to the left of a particular IPv6 Firewall rule configuration to update its parameters collectively.

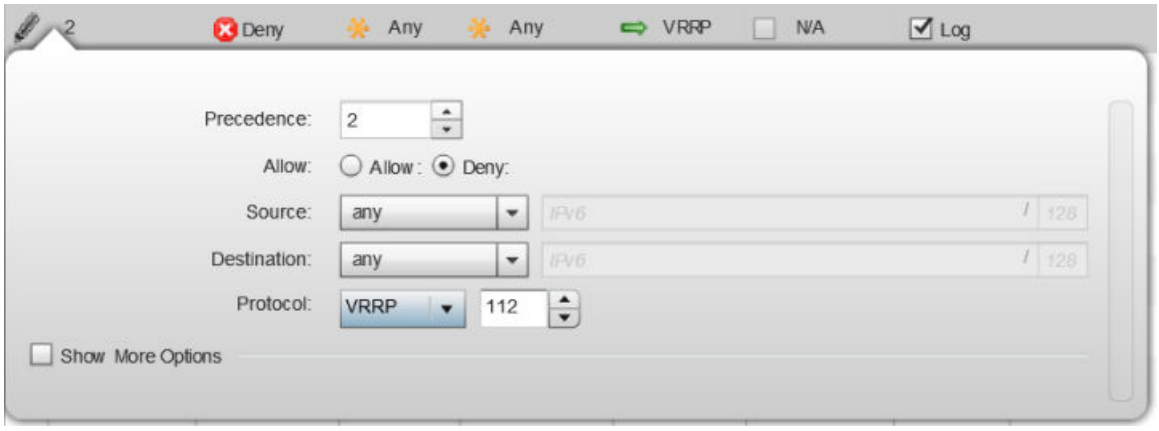



**Figure 290: WLAN Security - IPv6 Firewall Rules - Edit Rule Screen**

12 Click the icon in the **Description** column (top right-hand side of the screen) and select IPv6 filter values as needed to add criteria into the configuration of the IPv6 ACL.

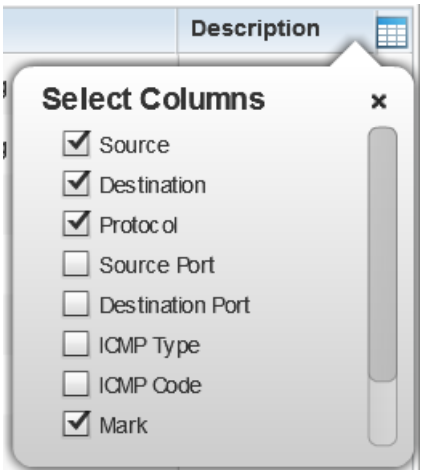



**Figure 291: WLAN Security - IPv6 Firewall Rules - IPv6 Firewall Rules Add Criteria Screen**

13 Define the following parameters for either inbound or outbound IPv6 firewall rules:

| | |
|---|---|
| Precedence | Specify or modify a precedence for this IPv6 policy between 1-1500. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.<br>The **Precedence** column sets the priority of a IPv6 Firewall rule within its rule set. |
| Action | Every IPv6 Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:<br>**Deny** Instructs the Firewall to prohibit a packet from proceeding to its destination<br>**Allow** Instructs the Firewall to allow a packet to proceed to its destination |
| Source | Select the source IPv6 address or network group configuration used as a basis matching criteria for this IPv6 ACL rule. Source options include:<br>• Any – Indicates any host device in any network.<br>• Network – Indicates all hosts in a particular IPv6 network. Subnet mask information must be provided for filtering based on network.<br>• Host – Indicates a single host with a specific IPv6 address. |
| Destination | Select the destination IPv6 address or network group configuration used as a basis matching criteria for this IPv6 ACL rule. Destination options include:<br>• Any – Indicates any host device in any network.<br>• Network – Indicates all hosts in a particular IPv6 network. Subnet mask information must be provided for filtering based on network.<br>• Host – Indicates a single host with a specific IPv6 address. |
| Protocol | Select the protocol to filter for this IPv6 ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number. |

| | |
|---|---|
| Source Port | If you are using either **tcp** or **udp** as the protocol, define whether the source port for incoming IPv6 ACL rule application is **any**, **equals**, or an administrator defined range. If you are not using **tcp** or **udp**, this setting displays as N/A. This is the data local origination port designated by the administrator. Selecting **equals** invokes a spinner control for setting a single numeric port.<br>Selecting **equals** invokes a spinner control for setting a single numeric port.<br>Selecting **range** displays spinner controls for low and high numeric range settings.<br>A source port cannot be a destination port. |
| Destination Port | If you are using either **tcp** or **udp** as the protocol, define whether the destination port for outgoing IPv6 ACL rule application is **any**, **equals**, or an administrator defined range. If you are not using **tcp** or **udp**, this setting displays as N/A. This is the data destination virtual port designated by the administrator.<br>Selecting **equals** invokes a spinner control for setting a single numeric port.<br>Selecting **range** displays spinner controls for low and high numeric range settings.<br>A source port cannot be a destination port. |
| ICMP Type | Selecting **ICMP** as the protocol for the IPv6 rule displays an additional set of ICMP specific options for ICMP type and code. The *Internet Control Message Protocol* (ICMP) uses messages identified by numeric type. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10. |
| ICMP Code | Selecting **ICMP** as the protocol for the IPv6 rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding code, helpful for troubleshooting network issues, for example *0 - Net Unreachable*, *1 - Host Unreachable*, and *2 - Protocol Unreachable*. |
| Mark | Select this option to mark certain fields inside a packet before allowing them. Mark applies only for **Allow** rules. Mark sets the rule's 802.1p or dscp level (from 0 - 7) |
| Log | Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed. |
| Description | Lists the administrator assigned description applied to the IPv6 ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a Select Columns screen used to add or remove IPv6 ACL criteria from the table. |

14 Click **OK** to save all changes to the IPv6 Firewall Rules dialog.

Click **Exit** to close the dialog and return to the previous screen.

15 Select existing inbound or outbound MAC Firewall Rules using the drop-down menu.

If no rules exist, select **Create** to display a screen where Firewall rules can be created.

16 Select the **+ Add Row** button.

17 Select the added row to expand it into configurable parameters.

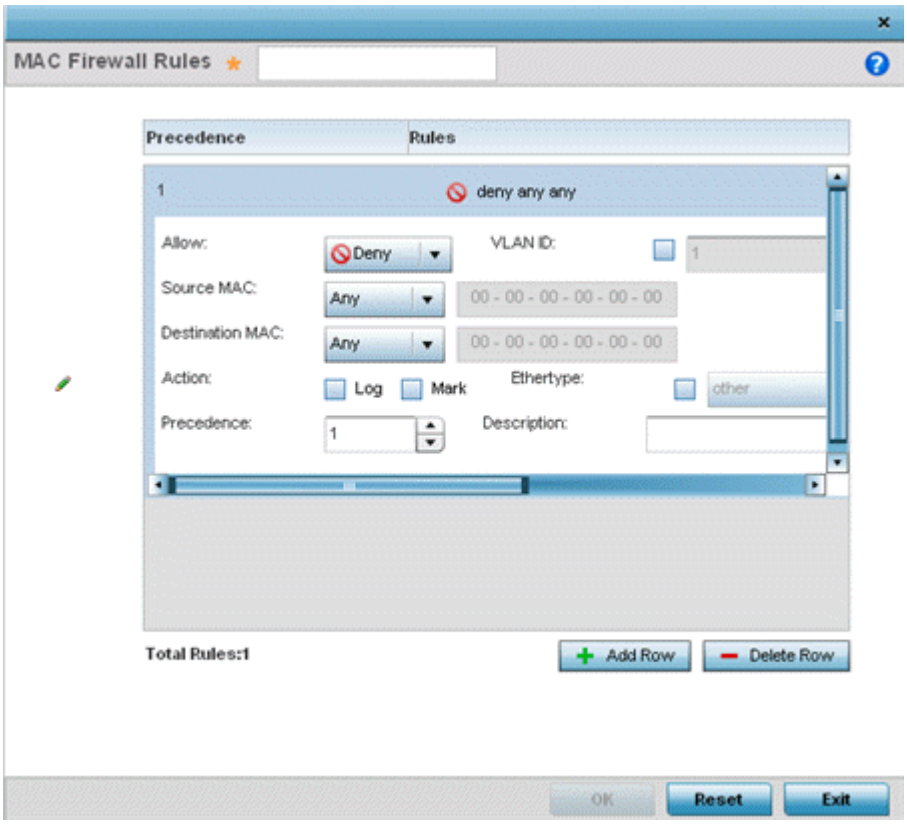



**Figure 292: WLAN Security - MAC Firewall Rules Screen**

18 Define the following parameters for either the inbound or outbound MAC Firewall Rules:

| | |
|---|---|
| Allow | Every IP Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:<br>**Deny** Instructs the Firewall to prohibit a packet from proceeding to its destination<br>**Permit** Instructs the Firewall to allow a packet to proceed to its destination |
| Source and Destination MAC | Enter both **Source** and **Destination** MAC addresses. The access point uses the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask. |
| Actions | The following actions are supported:<br>**Log** Creates a log entry that a Firewall rule has allowed a packet to either be denied or permitted.<br>**Mark** Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.<br>**Mark, Log** Conducts both mark and log functions. |
| Traffic Class | Sets an ACL traffic classification value for the packets identified by this inbound MAC filter. Traffic classifications are used for QoS purposes. Use the spinner to define a traffic class from 1- 10. |

| | |
|---|---|
| Precedence | Use the spinner control to specify a precedence for this MAC Firewall rule between 1-1500. Access policies with lower precedence are always applied first to packets. |
| VLAN ID | Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the access point's local RADIUS server). Set the VLAN form 1 - 4094. |
| Match 802.1P | Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting from 0 - 7. |
| Ethertype | Use the drop-down menu to specify an Ethertype of either **ipv6**, **arp**, **wisp** or **monitor 8021q**. An EtherType is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. When **other** is selected, the ethertype value can be configured manually. |
| Description | Provide an ACL setting description (up to 64 characters) for the rule to help differentiate it from others with similar configurations. |

19 Save the changes to the new MAC rule, or reset to the last saved configuration as needed.

20 Select the **+ Add Row** button.

21 Define the following parameters for **Association ACL**.

An Association ACL defines the rules used to allow/deny association to devices for this wireless LAN. If no Association ACL exists, select the **Create** button to display a new window where new ACL can be created.

| | |
|---|---|
| Precedence | Enter a numerical value indicating the precedence of rule execution. |
| Starting MAC Address | Enter a MAC address to define the start of range. This field is mandatory. |
| Ending MAC Address | Enter a MAC address to define the end of range. |
| Allow/Deny | Every Association ACL rule consists of matching criteria rules. The action defines what to do with the device if it matches the specified criteria. The following actions are supported:<br>**Deny** Instructs the Firewall to prevent the device from associating with this WLAN<br>**Permit** Instructs the Firewall to allow the device to associate with this WLAN |

22 Assign an **Application Policy** to the firewall and set the following metadata extraction rules:

| | |
|---|---|
| Application Policy | Use the drop-down menu to assign an application policy to the WLAN's firewall configuration. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that application. An application policy defines the rules or actions executed on recognized HTTP, SSL and .voice/video applications. For more information, refer to Application. |
| Voice/Video Metadata | Select this option to enable the extraction of voice and video metadata flows. When enabled, administrators can track voice and video calls by extracting parameters (packets transferred and lost, jitter, audio codec and application name). Most Enterprise VoIP applications like Facetime, Skype for Business, and VoIP terminals can be monitored for call quality and visualized on the Extreme NSight UI in manner similar to HTTP and SSL. Call quality and metrics can be determined only from calls that are established as unencrypted. This setting is disabled by default.<br>Note:<br>Starting with WiNG 5.9.3, NSight is a separate target. For information on Extreme NSight™, refer to the Extreme NSight User Guide available at https://extremenetworks.com/documentation. |

| | |
|---|---|
| HTTP Metadata | Select this option to enable the extraction of HTTP flows. When enabled, administrators can track HTTP Websites accessed by both internal and guest clients and visualize HTTP data usage, hits, active time and total clients on the Extreme NSight UI. This setting is disabled by default.<br><br>Note:<br>Starting with WiNG 5.9.3, NSight is a separate target. For information on Extreme NSight™, refer to the Extreme NSight User Guide available at https://extremenetworks.com/documentation. |
| SSL Metadata | Select this option to enable the extraction of SSL flows. When enabled, administrators can track SSL Websites accessed by both internal and guest clients and visualize SSL data usage, hits, active time and total clients on the Extreme NSight UI. This setting is disabled by default.<br><br>Note:<br>Starting with WiNG 5.9.3, NSight is a separate target. For information on Extreme NSight™, refer to the Extreme NSight User Guide available at https://extremenetworks.com/documentation. |

23 Set the following **Trust Parameters**:

| | |
|---|---|
| ARP Trust | Select this option to enable ARP trust on this WLAN. ARP packets received on this WLAN are considered trusted and information from these packets is used to identify rogue devices within the network. This setting is disabled by default. |
| Validate ARP Header Mismatch | Select this option to check for a source MAC mismatch in the ARP header and Ethernet header. This setting is enabled by default. |
| DHCP Trust | Select this option to enable DHCP trust on this WLAN. This setting is disabled by default. |

24 Set the following **IPv6 Settings**:

| | |
|---|---|
| ND Trust | Select this option to enable the trust of neighbor discovery requests on an IPv6 supported firewall on this WLAN. This setting is disabled by default. |
| Validate ND Header Mismatch | Select this option to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This setting is enabled by default. |
| DHCPv6 Trust | Select this option to enable the trust all DHCPv6 responses on this WLAN's firewall. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default |
| RA Guard | Select this option to enable router advertisements or ICMPv6 redirects on this WLAN's firewall. This setting is disabled by default. |

25 Set the following **Wireless Client Deny** configuration:

| | |
|---|---|
| Wireless Client Denied Traffic Threshold | When this option is enabled, any associated client, exceeding the thresholds configured for storm traffic, is either deauthenticated or blacklisted depending on the selected action. The threshold range is from 1- 1000000 packets per second. This feature is disabled by default. |
| Action | If you are enabling a wireless client threshold, use the drop-down menu to determine whether clients are deauthenticated when the threshold is exceeded, or blacklisted from connectivity for a user-defined interval. Selecting None applies no consequence to an exceeded threshold. |
| Blacklist Duration | Select this option and define a setting from 0 - 86,400 seconds. Offending clients can reauthenticate, once this blacklist duration has been exceeded. |

26 Set a **Firewall Session Hold Time** in either Seconds (1 - 300) or Minutes (1 - 5).

This is the hold time for caching user credentials and Firewall state information when a client roams. The default setting is 30 seconds.

27 Click **OK** when completed to update this WLAN's Firewall settings.

Click **Reset** to revert the screen to its last saved configuration.

Before defining an access control configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

## Configuring WLAN Client Settings

Each WLAN can maintain its own client setting configuration. These settings include wireless client inactivity timeouts and broadcast configurations.

Access points can support up to 256 clients each. Client load balancing can be enforced for the WLAN as more and more WLANs are deployed.

To define a WLAN's unique client support configuration:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.

2 Click **Add** to create an additional WLAN, or select and existing WLAN and click **Edit** to modify its properties.

3 Select the **Client Settings** tab.

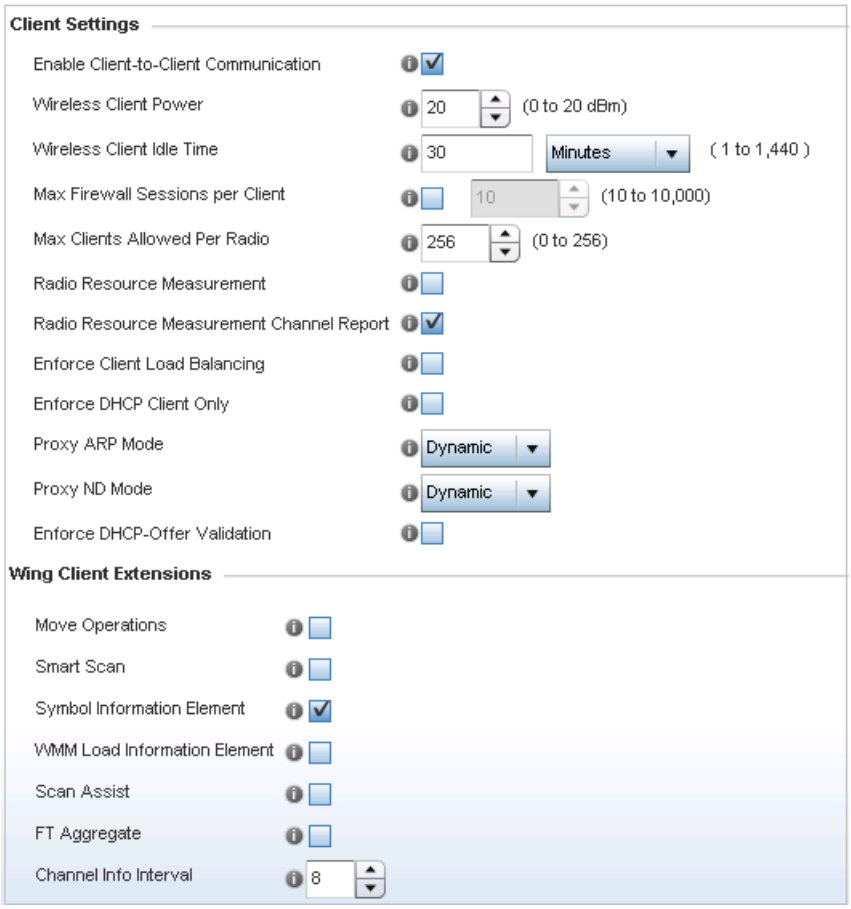



**Figure 293: WLAN Policy Client Settings Screen**

4 Define the following **Client Settings** for the WLAN:

| | |
|---|---|
| Enable Client-to-Client Communication | Select this option to enable client to client communication within this WLAN. The default is enabled, meaning clients are allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting also disabled on that WLAN, clients are not permitted to interoperate. |
| Wireless Client Power | Use this parameter to set the maximum transmit power (between 0 - 20 dBm) communicated to wireless clients for transmission within the network. The default value is 20 dBm. |
| Wireless Client Idle Time | Set the maximum amount of time wireless clients are allowed to be idle within this WLAN. Set the idle time in either Seconds (60 - 86,400), Minutes (1 - 1,440), Hours (0 - 24), or Days (0 - 1). When this setting is exceeded, the client is no longer able to access resources and must re-authenticate. The default value is 1,800 seconds. |
| Max Firewall Sessions per Client | Select this option to set the maximum amount of sessions (between 10 - 10,000) clients within the network over the Firewall. When enabled, this parameter limits the number of simultaneous sessions allowed by the Firewall per wireless client. This feature is disabled by default. |
| Max Clients Allowed Per Radio | Select this option to set the maximum number of clients (from 1- 256 clients) allowed to connect using a single radio. When enabled, this parameter limits the number of clients that are allowed to connect to a single radio. This feature is set to 256 by default. |

| | |
|---|---|
| Radio Resource Measurement | Select this option to enable radio resource measurement capabilities (IEEE 802.11k) on this WLAN. 802.11k improves how traffic is distributed. In a WLAN, each device normally connects to an access point with the strongest signal. Depending on the number and locations of the clients, this arrangement can lead to excessive demand on one access point and underutilization for others, resulting in degradation of overall network performance.<br>With 802.11k, if the access point with the strongest signal is loaded to its capacity, a client connects to a underutilized access point. Even if the signal is weaker, the overall throughput is greater since it's an efficient use of the network's resources. This setting is disabled by default. |
| Radio Resource Measurement Channel Report | Select this option to enable radio resource measurement channel reporting (IEEE 802.11k) on this WLAN. This setting is disabled by default. |
| Enforce Client Load Balancing | Select this option to distribute clients evenly amongst associated access point radios. This feature is disabled by default. Client load balancing can be enforced for the WLAN as more and more WLANs are deployed.<br>Loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another access point radio. |
| Enforce DHCP Client Only | Select the check box to enforce that the firewall allows packets from clients only if they used DHCP to obtain an IP address, disallowing static IP addresses. This feature is disabled by default. |
| Proxy ARP Mode | Use the drop-down menu to define the proxy ARP mode as either **`Strict`** or **`Dynamic`**. Proxy ARP is the technique used by the access point to answer ARP requests intended for another system. By faking its identity, the access point accepts responsibility for routing packets to the actual destination. Dynamic is the default value. |
| Enforce DHCP-Offer Validation | Select the check box to enforce DHCP offer validation. The default setting is disabled. |

5 Define the following **Wing Client Extensions** for the WLAN:

| | |
|---|---|
| Move Operations | Select the check box to enable the use of HFSR *(Hyper-Fast Secure Roaming)* for clients on this WLAN. This feature applies only to certain client devices and is disabled by default. |
| Smart Scan | Enable a smart scan to refine a clients channel scans to just a few channels as opposed to all available channels. This feature is disabled by default. |
| Symbol Information Element | Select the check box to support the Symbol Information Element with legacy Symbol Technology clients, thus making them optimally interoperable with the latest Extreme Networks access points. The default setting is enabled. |
| WMM Load Information Element | Select the check box to support a WMM Load Information Element in radio transmissions with legacy clients. The default setting is disabled. |
| Scan Assist | Enable scan assist to achieve faster roams on DFS channels by eliminating passive scans. Clients would get channel information directly from possible roam candidates. This setting is disabled by default. |

| | |
|---|---|
| FT Aggregate | Enable FT *(fast transition)* aggregate to increase roaming speed by eliminating separate key exchange handshake frames with potential roam candidates. Enable fast transition to complete an initial FT over DS handshake with multiple roam candidates (up to 6) at once, eliminating the need to send separate FT over DS handshakes to each roam candidate. This setting is disabled by default. |
| Channel Info Interval | Configure the channel information interval to periodically retrieve channel information directly from potential roam candidates without making a scan assist request. |

6 Define the following **Coverage Hole Detection** settings to determine how detected coverage holes are managed:

| | |
|---|---|
| Enable | Enable this setting to inform an access point when it experiences a coverage hole (area of poor wireless coverage). This setting is disabled by default. |
| Use 11k Clients | Optionally enable this setting to also use 802.11k-only-capable clients to detect coverage holes. This is a reduced set of coverage hole detection capabilities (only standard 11k messages and behaviors). This setting is disabled by default. |
| Threshold | Use the spinner control to set the access point signal strength (as seen by the client) below which a coverage hole incident is reported. The threshold can be set from -80 to -60. |
| Offset | Use the spinner control to set the offset added to the threshold to obtain the access point signal strength (as seen by the client) considered adequate. The offset can be set from 5 to 20. |

7 Set the following **AP Attributes Information**:

| | |
|---|---|
| Enable | Select this option to include the AP-Attributes information element in the beacon. The information element helps clients recognize which wing-extensions are supported by the AP. This setting is enabled by default. |
| Include Hostname | Select this option to include the AP's hostname in the AP-Attributes information element. This setting is disabled by default. |

8 Define the following **Timeout Settings** for the WLAN:

| | |
|---|---|
| Credential Cache Timeout | Set a timeout period for the credential cache in Days (0-1), Hours (0-24), Minutes (1-1440), or Seconds (60-86,4000). The default setting is 1 hour. |
| VLAN Cache Timeout | Set a timeout period for the VLAN cache in Days (0-1), Hours (0-24), Minutes (1-1440), or Seconds (60-86,4000). The default setting is 1 hour. |

9 Select **Controller Assisted Mobility** to use a controller or service platform's mobility database to assist in roaming between RF Domains. This feature is disabled by default.

10 Use the **Device ID** settings, within the **OpenDNS** field, to specify a 16 character maximum OpenDNS device ID forwarded in a DNS query. OpenDNS extends DNS by adding additional features such as misspelling correction, phishing protection, and optional content filtering.

11 Click **OK** when completed to update the WLAN's client settings. Click **Reset** to revert the screen to the last saved configuration.

## Configuring WLAN Accounting Settings

Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets and number of bytes. Accounting enables wireless network administrators to track the services

users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports and logs user activity to a RADIUS security server in the form of accounting records. Each accounting record is stored on a local access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA.

Accounting can be enabled and applied to WLANs, to uniquely log accounting events specific to the WLAN. Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to an external location for periodic network and user permission administration.

To configure WLAN accounting settings:

1 Select **Configuration → Wireless → Wireless LANs** to display available WLANs.
2 Click **Add** to create an additional WLAN, or select and existing WLAN and click **Edit** to modify its properties.
3 Select **Accounting**.

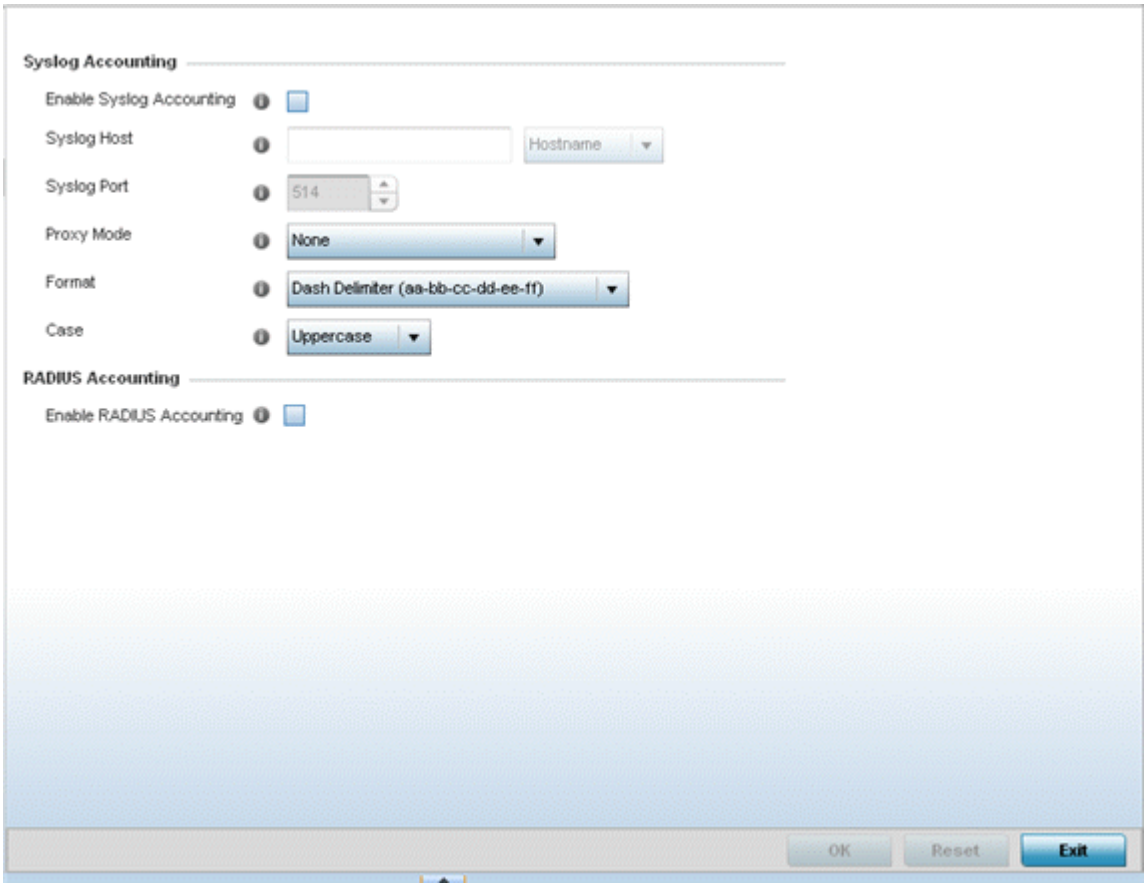



**Figure 294: WLAN Accounting Screen**

4 Set the following **Syslog Accounting** information:

| | |
|---|---|
| Enable Syslog Accounting | Use this option to generate accounting records in standard syslog format (RFC 3164). The feature is disabled by default. |
| Syslog Host | Use the drop-down menu to select either **Hostname** or **IP Address**. Based on th eoption you have selected, specify the IP address or hostname of the external syslog host where accounting records are routed.<br>Note:<br>Hostnames cannot include an underscore character. |
| Syslog Port | Use the spinner control to set the destination UDP port number of the external syslog host where the accounting records are routed. The default port is 514. |
| Proxy Mode | If a proxy is needed to connect to the syslog server, choose a proxy mode of **Through RF Domain Manager** or **Through Wireless Controller.** If no proxy is needed, select **None**. |
| Format | Specify the delimiter format for the MAC address to be packed in the syslog request. Available formats are **No Delimiter** (aabbccddeeff), **Colon Delimiter** (aa:bb:cc:dd:ee:ff), **Dash Delimiter** (aa-bb-cc-dd-ee-ff), **Dot Delimiter** (aabb.ccdd.eeff) and **Middle Dash Delimiter** (aabbcc-ddeeff). |
| Case | Specify to send the MAC addresses in either **Uppercase** or **Lowercase** for syslog requests. The default setting is **Uppercase**. |

5 Select the **Enable RADIUS Accounting** check box to use an external RADIUS resource for AAA accounting. When the check box is selected, an **AAA Policy** field displays. Either use the default AAA policy with the WLAN, or select **Create** to define a new AAA configuration that can be applied to the WLAN. This setting is disabled by default.

6 Click **OK** when completed to update the WLAN's accounting settings. Click **Reset** to revert the screen to the last saved configuration.

*Accounting Deployment Considerations*

Before defining a WLAN AAA configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- When using RADIUS authentication, the WAN port round trip delay should not exceed 150ms. Excessive delay over a WAN can cause authentication and roaming issues. When excessive delays exists, a distributed RADIUS service should be used.
- Authorization policies should be implemented when users need to be restricted to specific WLANs, or time and date restrictions need to be applied.
- Authorization policies can also apply bandwidth restrictions and assign Firewall policies to users and devices.

## Configuring WLAN Service Monitoring Settings

Service Monitoring is a mechanism for administrating external AAA server, captive portal server, access point adoption, and DHCP server activity for WLANs. Service monitoring enables an administrator to better notify users of a service's availability and make resource substitutions. Service monitoring can be enabled and applied to log activity as needed for specific WLANs.

External services can be rendered unavailable due to any of the following instances:

- When the RADIUS authentication server becomes unavailable. The RADIUS server could be local or external to the controller, service platform or access point.
- When an externally hosted captive portal is unavailable (for any reason)
- If an access point's connected controller or service platform becomes unavailable.
- When a monitored DHCP server becomes unavailable.

To configure Service Monitoring settings:

1 Select **Configuration → Wireless → Wireless LANs** to display a high-level display of the existing WLANs.
2 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.
3 Click **Service Monitoring**.

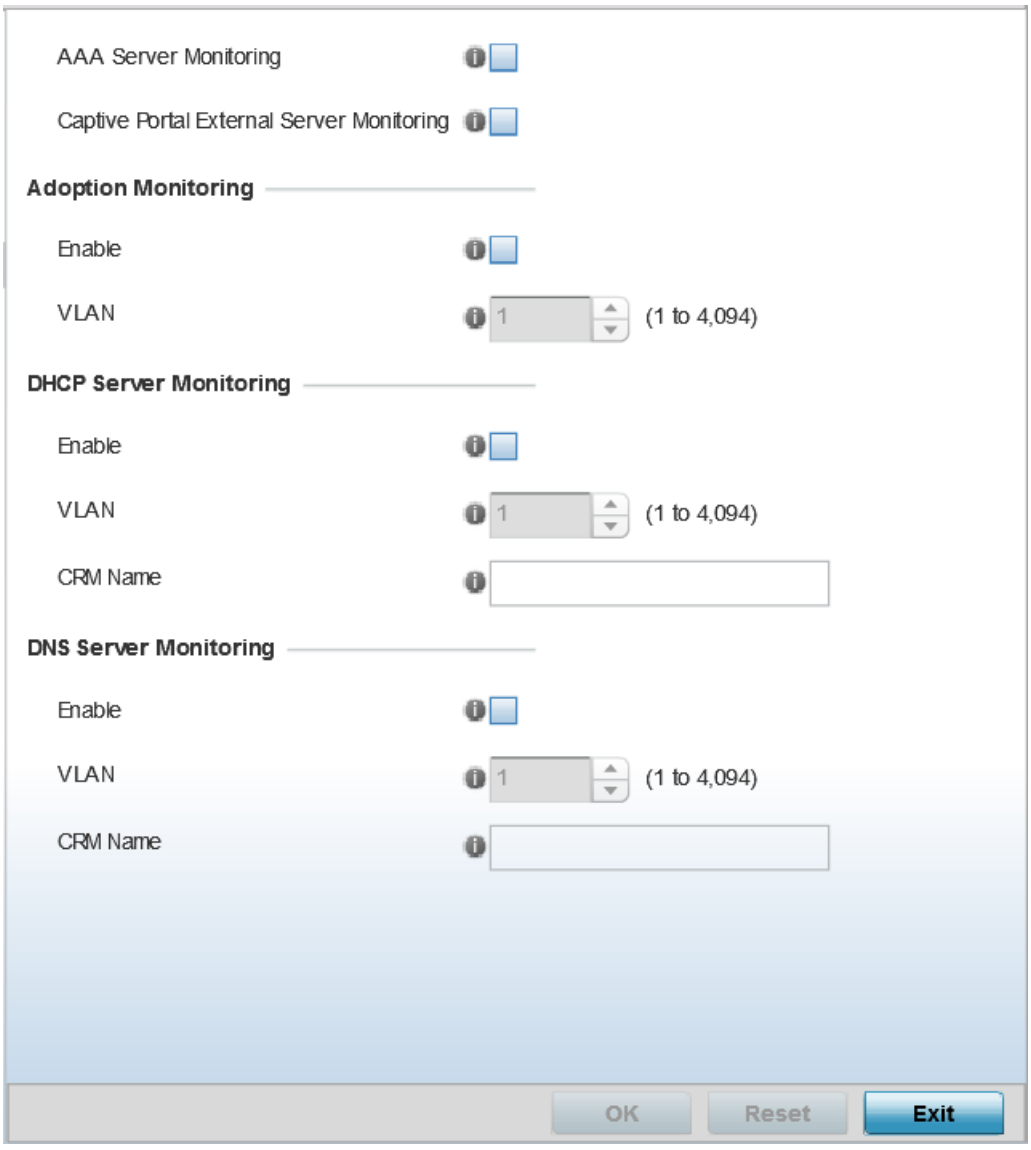



**Figure 295: WLAN Policy Service Monitoring Screen**

4 Select **AAA Server monitoring** to monitor a dedicated external RADIUS server and ensure its adoption resource availability.

This setting is disabled by default.

5 Select **Captive Portal External Server monitoring** to monitor externally hosted captive portal activity, and to set temporary and restrictive user access to the controller or service platform managed network.

This setting is disabled by default.

6 Refer to the **Adoption Monitoring** field to set the WLAN's adoption service monitoring configuration.

| | |
|---|---|
| Enable | Select this option to verify access points' adoption status to their controllers or service platform. When the connection is lost, captive portal users are automatically migrated to the VLAN defined in the **VLAN** field. This option is disabled by default. |
| VLAN | Select the VLAN to which users are migrated when an access point's connection to its adopting controller or service platform is lost. The available range is from 1 to 4,094. |

7 Refer to the **DHCP Server Monitoring** field to set the WLAN's adoption service monitoring configuration.

| | |
|---|---|
| Enable | Select to enable monitoring of the configured DHCP server. When the connection to the monitored DHCP server is lost, all captive portal data users are automatically migrated to the VLAN defined in the **VLAN** field.<br>Note:<br>This option is disabled by default. |
| VLAN | Select the VLAN to which users are migrated when the configured DHCP server becomes available. The available range is from 1 to 4,094. |
| CRM Name | Enter the name of the DHCP server to monitor for availability. When this DHCP server resource becomes unavailable, the device falls back to the defined VLAN. This VLAN has a DHCP server configured that provides a pool of IP addresses and with a lease time less than the main DHCP server. |

8 Refer to the **DNS Server Monitoring** field to set the WLAN's adoption service monitoring configuration.

| | |
|---|---|
| Enable | Select to enable monitoring of the configured DNS server. When the connection to the monitored DNS server is lost, all captive portal data users are automatically migrated to the VLAN defined in the **VLAN** field. This option is disabled by default. |
| VLAN | Select the VLAN to which users are migrated when the configured DNS server becomes available. The available range is from 1 to 4,094. |
| CRM Name | Enter the name of the DNS server to monitor for availability. When this DNS server resource becomes unavailable, the device falls back to the defined VLAN. This VLAN has a DNS server configured that provides DNS address resolution until the primary DNS server becomes available. |

9 Click **OK** when completed to update this WLAN's service monitor settings.

Click **Reset** to revert the screen to its last saved configuration.

## Configuring Client Load Balancing Settings

Client load balance settings can be defined generically for both the 2.4 GHz and 5.0 GHz bands, and specifically for either of the 2.4 GHz or 5.0 GHz bands.

To configure client load balancing settings on an access point managed WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display a high-level display of the existing WLANs.

2 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.

3 Select **Client Load Balancing**.

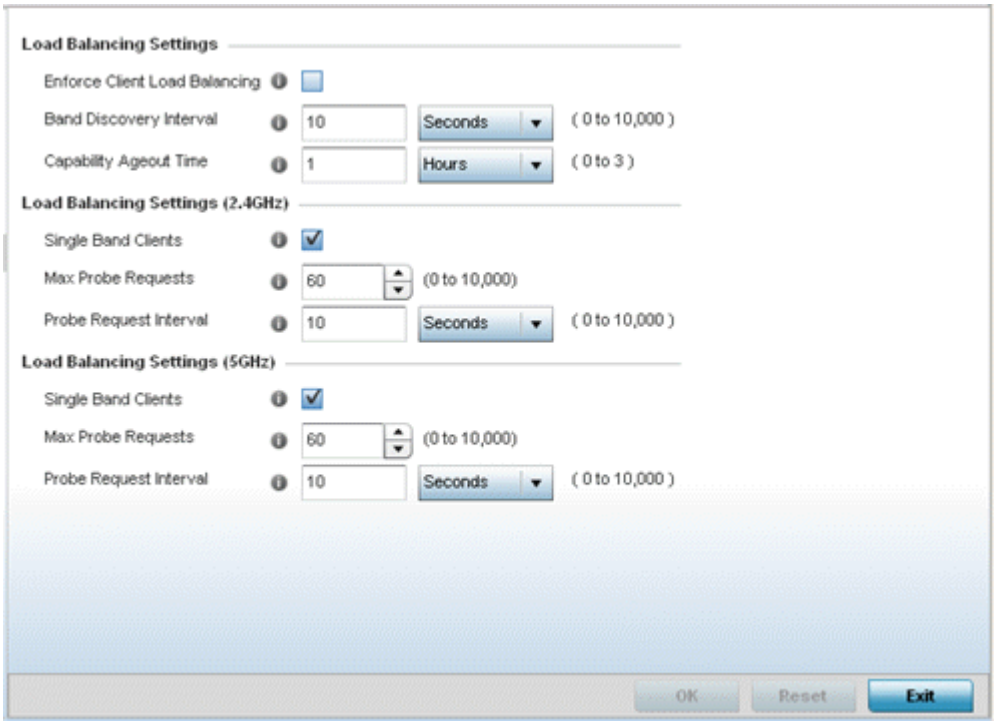



**Figure 296: WLAN Policy Client Load Balancing Screen**

4 Refer to the **Load Balancing Settings** section to configure load balancing for the WLAN. These settings are generic to both the 2.4 GHz and 5.0 GHz bands.

| | |
|---|---|
| Enforce Client Load Balancing | Select this option to enforce a client load balance distribution on this WLAN's access point radios.<br>The following models can support 256 clients per access point: AP 6522, AP 6532, AP 6562, AP 7161, AP 7602, AP 7622, AP 81XX.<br>The following models can support 512 clients per access point: AP-7612, AP7632, AP7662.<br>Loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another access point radio. This setting is enabled by default.. |
| Band Discovery Interval | Define a value in either seconds (0 - 10,000), minutes (0 -166) or hours (0 - 2) the access point uses to discover a client's band capabilities before associating. The default setting is 10 seconds. |
| Capability Ageout Time | Define a value in either seconds (0 - 10,000), minutes (0 -166) or hours (0 -2) to ageout a client's capabilities from the internal table.<br>The default is 1 hour. |

5 Refer to the **Load Balancing Settings (2.4GHz)** field to configure load balancing for the 2.4 GHz WLAN.

| | |
|---|---|
| Single Band Clients | Select this option to enable association for single 2.4GHz clients, even if load balancing is available. This setting is enabled by default. |
| Max Probe Requests | Enter a value from 0 - 10,000 for the maximum number of probe requests for clients using the 2.4GHz frequency. The default value is 60. |
| Probe Request Interval | Enter a value in seconds from 0 - 10,000 to set an interval for client probe requests, beyond which association is allowed for clients on the 2.4 GHz frequency. The default is 10 seconds. |

6 Refer to the **Load Balancing Settings (5GHz)** field to configure load balancing for the 5GHz WLAN.

| | |
|---|---|
| Single Band Clients | Select this option to enable the association of single 5GHz clients, even if load balancing is available. This setting is enabled by default. |
| Max Probe Requests | Enter a value from 0 - 10,000 for the maximum number of client associations on the 5.0 GHz frequency. The default value is 60. |
| Probe Request Interval | Enter a value in seconds from 0 - 10,000 to configure the interval for client probe requests. When exceeded, clients can associate in 5GHz. The default is 10 seconds. |

7 Click **OK** when completed to update this WLAN's client load balance settings.

Click **Reset** to revert the screen to its last saved configuration.

## Configuring Advanced WLAN Settings

1 Select **Configuration → Wireless → Wireless LANs** to display a high-level display of the existing WLANs.

2 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.

3 Click **Advanced**.

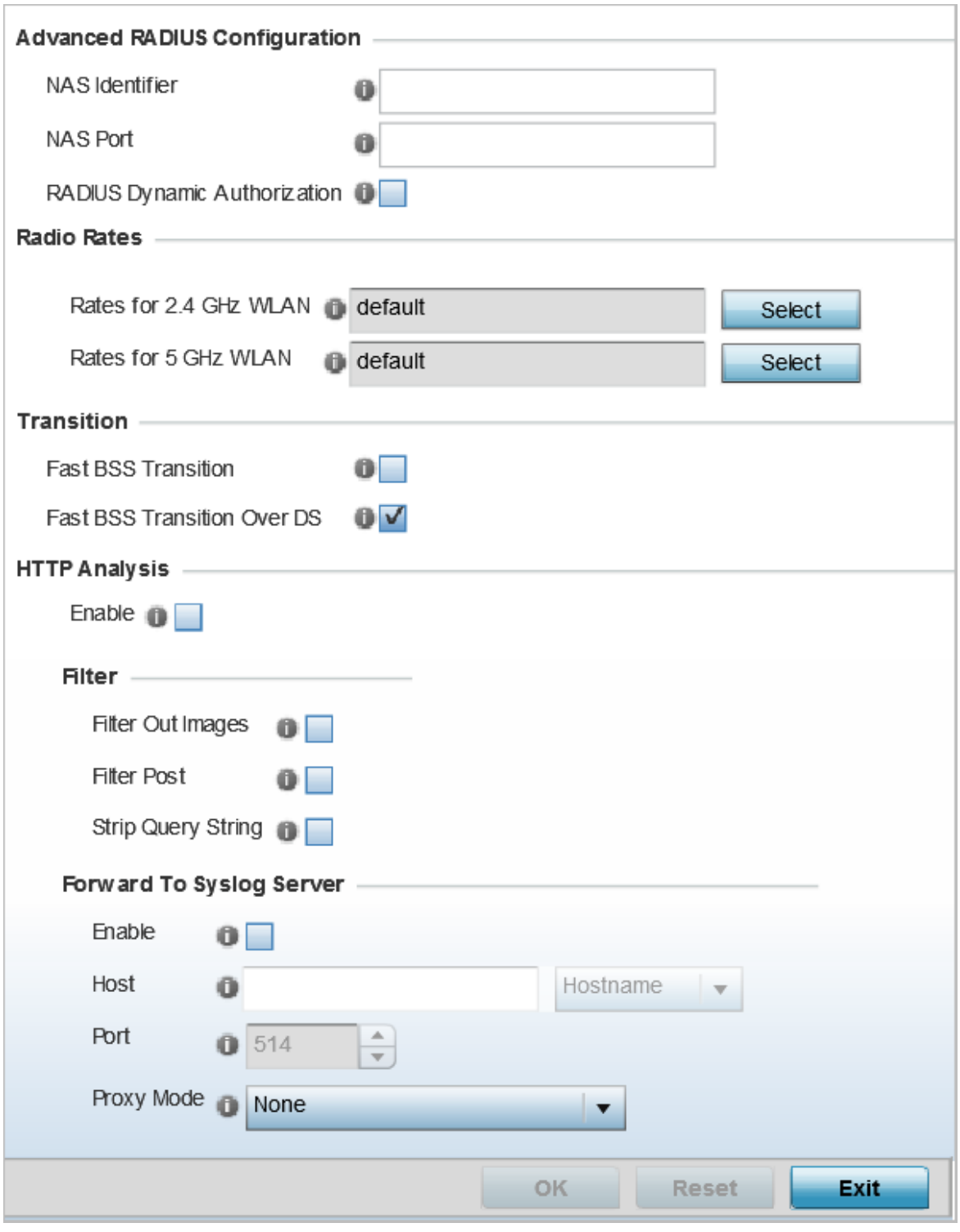



**Figure 297: WLAN - Advanced Configuration Screen**

4 Refer to the **Advanced RADIUS Configuration** field to set the WLAN's NAS configuration and RADIUS Dynamic Authorization.

| | |
|---|---|
| NAS Identifier | Specify what is included in the RADIUS NAS-Identifier field for authentication and accounting packets. This is an optional setting, and defaults are used if no values are provided. |
| NAS Port | The profile database on the RADIUS server consists of user profiles for each connected NAS *(network access server)* port. Each profile is matched to a user name representing a physical port. When the access point authorizes users, it queries the user profile database using a user name representative of the physical NAS port making the connection. |
| RADIUS Dynamic Authorization | Select this check box to enable the RADIUS protocol to support unsolicited messages sent from the RADIUS server. These messages allow administrators to issue CoA *(change of authorization)* messages, which affect session authorization, or DM *(Disconnect Messages)*, which cause a session to terminate immediately. This option is disabled by default. |

5 Refer to the **Radio Rates** field to define selected data rates for both the 2.4 GHz and 5.0 GHz bands.

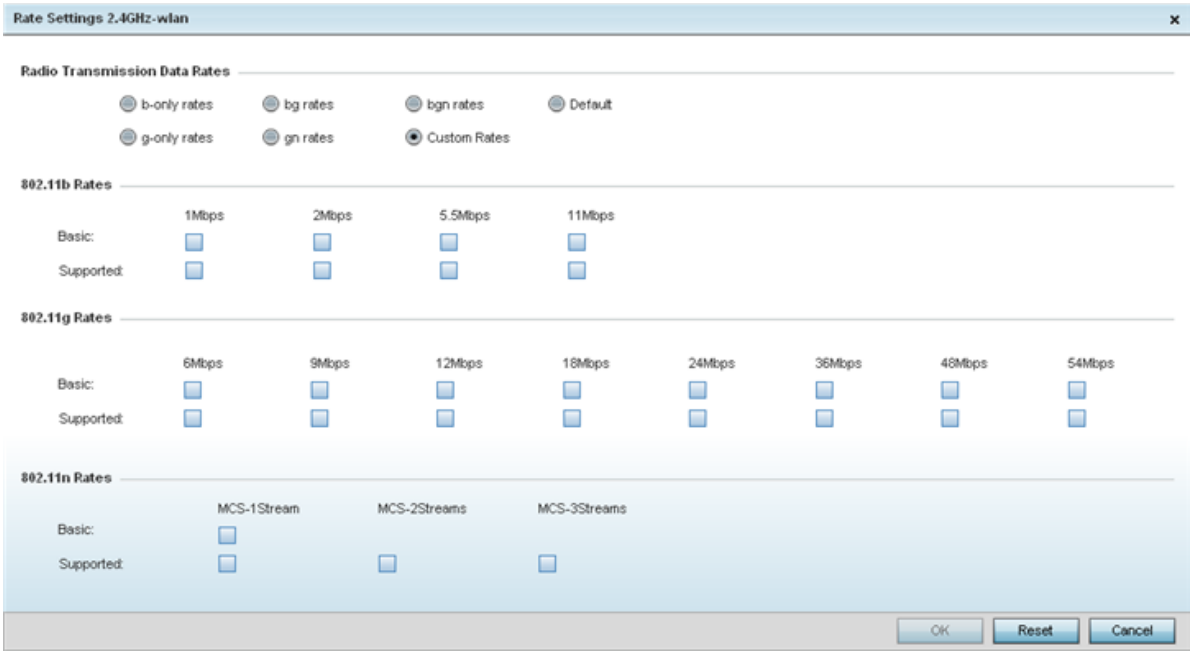



**Figure 298: Advanced WLAN Rate Settings 2.4 GHz Screen**

For 2.4 GHz WLAN radio transmission rate settings, define the minimum basic and supported rates in the **802.11b Rates**, **802.11g Rates** and **802.11n Rates** sections. These rates are applicable to client traffic associated with this WLAN only.

If supporting 802.11n, select a Supported MCS index. Set an MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

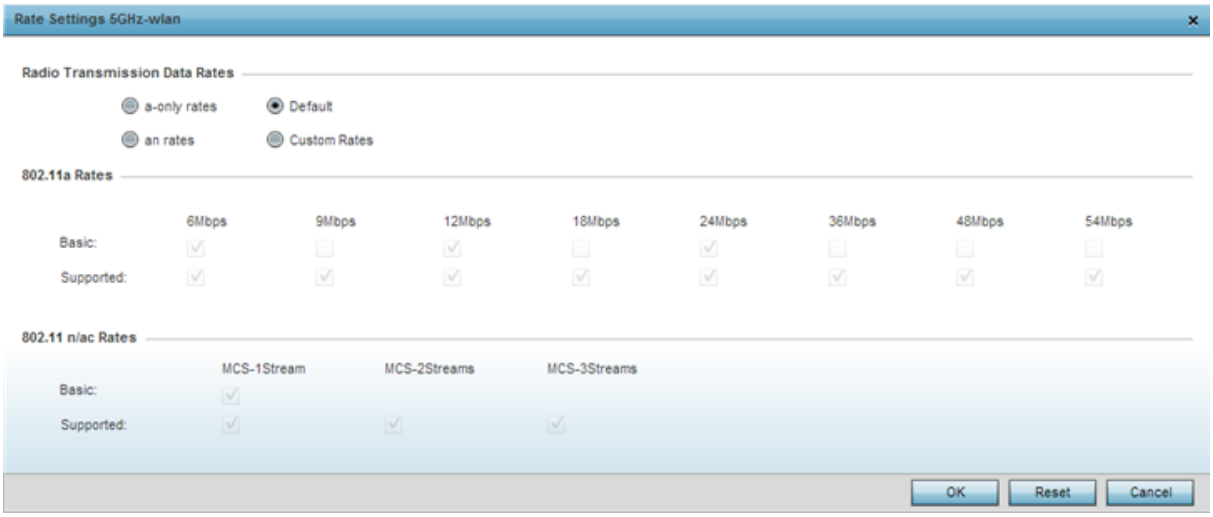



**Figure 299: Advanced WLAN Rate Settings 5 GHz Screen**

For 5.0 GHz WLAN radio transmission rate settings, define the minimum basic and supported rates in the **802.11b Rates** and **802.11n Rates** sections. These rates are applicable to client traffic associated with this WLAN only.

If supporting 802.11n, select a Supported MCS index. Set an MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

802.11n MCS rates are defined as follows, both with and without short guard intervals (SGI):

**Table 6: MCS-1 Stream**

| MCS Index | Number of Streams | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI |
|---|---|---|---|---|---|
| 0 | 1 | 6.5 | 7.2 | 13.5 | 15 |
| 1 | 1 | 13 | 14.4 | 27 | 30 |
| 2 | 1 | 19.5 | 21.7 | 40.5 | 45 |
| 3 | 1 | 26 | 28.9 | 54 | 60 |
| 4 | 1 | 39 | 43.4 | 81 | 90 |
| 5 | 1 | 52 | 57.8 | 108 | 120 |
| 6 | 1 | 58.5 | 65 | 121.5 | 135 |
| 7 | 1 | 65 | 72.2 | 135 | 150 |

**Table 7: MCS-2 Stream**

| MCS-2Stream Index | Number of Streams | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI |
|---|---|---|---|---|---|
| 0 | 2 | 13 | 14.4 | 27 | 30 |
| 1 | 2 | 26 | 28.9 | 54 | 60 |
| 2 | 2 | 39 | 43.4 | 81 | 90 |
| 3 | 2 | 52 | 57.8 | 108 | 120 |
| 4 | 2 | 78 | 86.7 | 162 | 180 |
| 5 | 2 | 104 | 115.6 | 216 | 240 |
| 6 | 2 | 117 | 130 | 243 | 270 |
| 7 | 2 | 130 | 144.4 | 270 | 300 |

**Table 8: MCS-3 Stream**

| MCS-3Stream Index | Number of Streams | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI |
|---|---|---|---|---|---|
| 0 | 3 | 19.5 | 21.7 | 40.5 | 45 |
| 1 | 3 | 39 | 43.3 | 81 | 90 |
| 2 | 3 | 58.5 | 65 | 121.5 | 135 |
| 3 | 3 | 78 | 86.7 | 162 | 180 |
| 4 | 3 | 117 | 130.7 | 243 | 270 |
| 5 | 3 | 156 | 173.3 | 324 | 360 |
| 6 | 3 | 175.5 | 195 | 364.5 | 405 |
| 7 | 3 | 195 | 216.7 | 405 | 450 |

802.11ac MCS rates are defined as follows, both with and without *short guard intervals* (SGI):

**Table 9: MCS-802.11ac (Theoretical Throughput for Single Spatial Streams)**

| MCS Index | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI | 80 MHz No SGI | 80 MHz With SGI |
|---|---|---|---|---|---|---|
| 0 | 6.5 | 7.2 | 13.5 | 15 | 29.3 | 32.5 |
| 1 | 13 | 14.4 | 27 | 30 | 58.5 | 65 |
| 2 | 19.5 | 21.7 | 40.5 | 45 | 87.8 | 97.5 |
| 3 | 26 | 28.9 | 54 | 60 | 117 | 130 |

**Table 9: MCS-802.11ac (Theoretical Throughput for Single Spatial Streams) (continued)**

| MCS Index | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI | 80 MHz No SGI | 80 MHz With SGI |
|---|---|---|---|---|---|---|
| 4 | 39 | 43.3 | 81 | 90 | 175.5 | 195 |
| 5 | 52 | 57.8 | 108 | 120 | 234 | 260 |
| 6 | 58.5 | 65 | 121.5 | 135 | 263.3 | 292.5 |
| 7 | 65 | 72.2 | 135 | 150 | 292.5 | 325 |
| 8 | 78 | 86.7 | 162 | 180 | 351 | 390 |
| 9 | N/A | N/A | 180 | 200 | 390 | 433.3 |

6 Set the following **Transition** options:

| | |
|---|---|
| Fast BSS Transition | If needed, select **Fast BSS Transition** to enable 802.11r fast roaming on this WLAN. This setting is disabled by default. 802.11r is an attempt to undo the burden that security and QoS added to the handoff process, and restore it to an original four message exchange process. The central application for the 802.11r standard is VOIP using mobile phones within wireless Internet networks. |
| Fast BSS Transition Over DS | Optionally select **Fast BSS Transition Over DS** to enable 802.11r over DS fast roaming on this WLAN. This setting is enabled by default. |

7 Enable **HTTP Analysis** for log file analysis on this WLAN.

This setting is disabled by default.

8 Set the following **Filter** settings for HTTP analysis on this WLAN:

| | |
|---|---|
| Filter Out Images | Select this option to filter images out of this WLAN's log files. This setting is disabled by default. |
| Filter Post | Select this option to filter posts out of this WLAN's log files. This setting is disabled by default. |
| Strip Query String | Select this option to filter query strings out of this WLAN's log files. This setting is disabled by default. |

9 Set the following **Forward to Syslog Server** settings for HTTP analysis on this WLAN:

| | |
|---|---|
| Enable | Select the check box to forward any firewall HTTP analytics to a specified syslog server for this WLAN. This setting is disabled by default. |
| Host | Provide a **`Hostname`** or **`IP Address`** of the remote syslog server. Use the drop-down menu to select the type of host address. |
| Port | Specify the port number utilized by the syslog server. The default port is 514. |
| Proxy Mode | If a proxy is needed to connect to the syslog server, select a proxy mode of either **`Through RF Domain Manager`** or **`Through Wireless Controller`**. If no proxy is needed, select **`None`**. |

10 Click **OK** when completed to update this WLAN's advanced settings.

Click **Reset** to revert the screen to its last saved configuration.

## Configuring Auto Shutdown Settings

Auto shutdown provides a mechanism to regulate the availability of a WLAN based on time. WLANs can be enabled or disabled depending on the day of the week and time of day.

A WLAN can be made available during a particular time of the day to prevent misuse and reduce the vulnerability of the wireless network. WLANs can be disabled when there are no users on the network, such as after hours or during the weekends/holidays. This enables the network administrator to have more time to manage the network as the mundane task of shutting down/staring up a WLAN is automated.

You can also use the Auto Shutdown screen to configure network parameters, which if not met, can force the WLAN to shut down. These parameters are:

- **`Shutdown on Mesh Point Loss`** – If an access point is a member in a meshed network and its connection to the mesh is lost, then all WLANs on the access point that have this option enabled are shut down.
- **`Shutdown on Primary Port Link Loss`** – When there is a loss of link on the primary wired link on the access point, all the WLANs on the access point that have this option enabled are shut down.
- **`Shutdown on Critical Resource Down`** – If critical resource monitoring is enabled on the access point and one or all of the monitored critical resource goes down, the all WLANs on the access point that have this option enabled are shut down.
- **`Shutdown on Unadoption`** – If the access point is unadopted from its wireless controller, then all WLANs on the access point that have this option enabled are shut down.

To configure auto shutdown for a WLAN:

1 Select **Configuration → Wireless → Wireless LANs** to display a high-level display of the existing WLANs.
2 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.
3 Select **Auto Shutdown**.

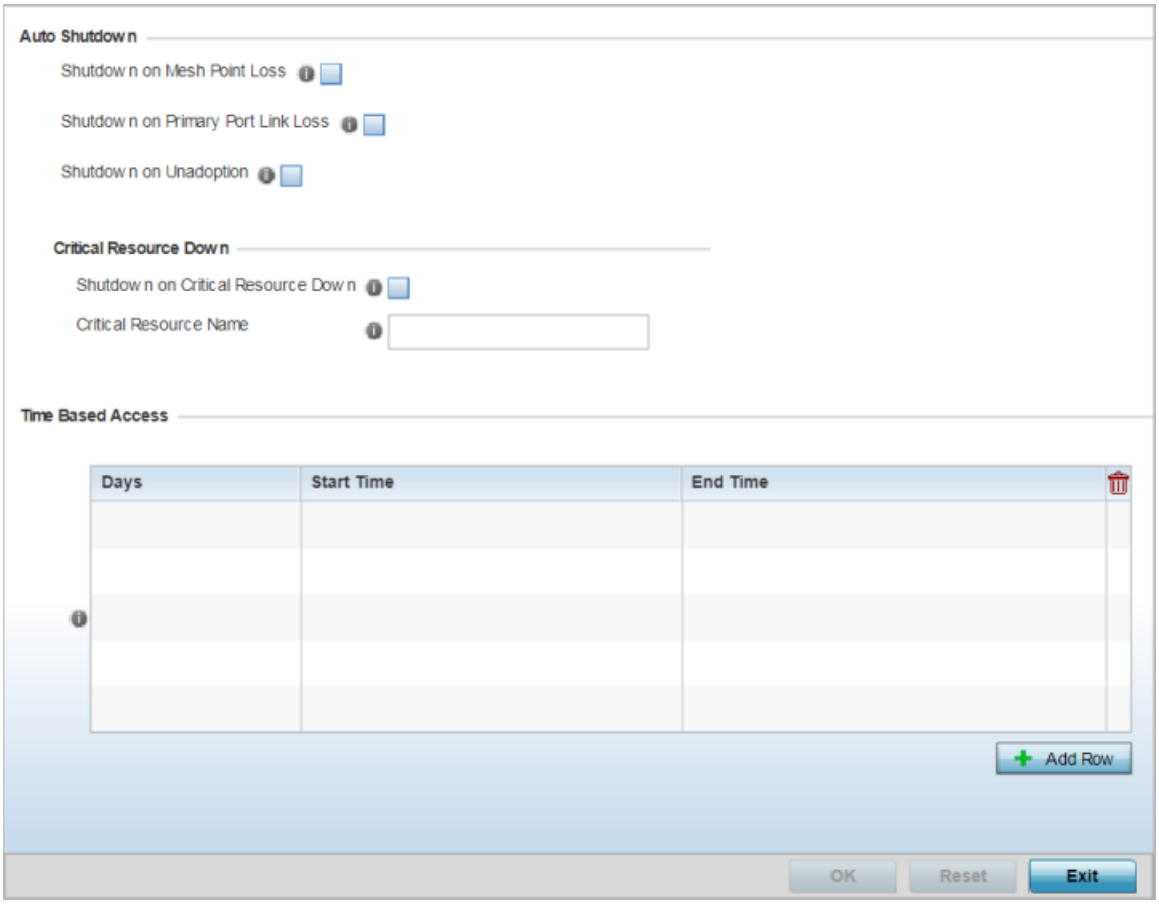



**Figure 300: WLAN - Auto Shutdown Screen**

4 Refer to the **Auto Shutdown** field to set the WLAN's shutdown criteria.

| | |
|---|---|
| Shutdown on Mesh Point Loss | Select to enable the WLAN to shutdown if the access point's connection to the mesh network is lost. This setting is disabled by default. |
| Shutdown on Primary Port Link Loss | Select to enable the WLAN to shutdown if the access point's connection on its primary wired port is lost. This setting is disabled by default. |
| Shutdown on Unadoption | Select to enable the WLAN to shutdown if the access point is unadopted from its wireless controller. This setting is disabled by default. |

5 Refer to the **Critical Resource Down** settings to determine whether a WLAN auto shutdown is enabled when a defined critical resource goes offline:

| | |
|---|---|
| Shutdown on Critical Resource Down | Select this option to automatically disable the WLAN when a defined critical resource goes offline. This setting is disabled by default. |
| Critical Resource Name | When enabled, enter a 127-character maximum critical resource name.This is the resource that must remain online to keep the selected WLAN online. |

6 To configure **Time Based Access** for this WLAN, click **+ Add Row** and configure each of the following options:

| | |
|---|---|
| Days | Select a day of the week to apply this access policy. Selecting **All** will apply the policy every day. Selecting **weekends** will apply the policy on Saturdays and Sundays only. Selecting **weekdays** will apply the policy on Monday, Tuesday, Wednesday, Thursday and Friday only. Selecting individual days of the week will apply the policy only on the selected day(s). |
| Start Time | This value sets the starting time the WLAN is activated. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose **AM** or **PM**. |
| End Time | This value sets the ending time of day(s) the WLAN is disabled. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose **AM** or **PM**. |

7 Click **OK** when completed to update this WLAN's auto shutdown settings. Click **Reset** to revert the screen to its last saved configuration.

## WLAN QoS Policies

QoS *(Quality of service)* provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories, for example **Video**, **Voice**, and **Data**. Packets within each category are processed based on the weights defined for each WLAN.

The Quality of Service screen displays a list of QoS policies available to WLANs. If none of the exiting QoS policies supports an ideal QoS configuration for the intended data traffic of this WLAN, click **Add** to create new policy. Select the radio button of an existing WLAN and click **OK** to map the QoS policy to the WLAN displayed in the banner of the screen.

Use the WLAN Quality of Service (QoS) Policy screen to add a new QoS policy or edit the attributes of an existing policy. Each access point model supports up to 32 WLAN QoS policies.

Note
WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radios themselves, independent from the wireless clients the access point radios supported.

1 Select **Configuration → Wireless → WLAN QoS Policy** to display existing QoS policies available to WLANs.

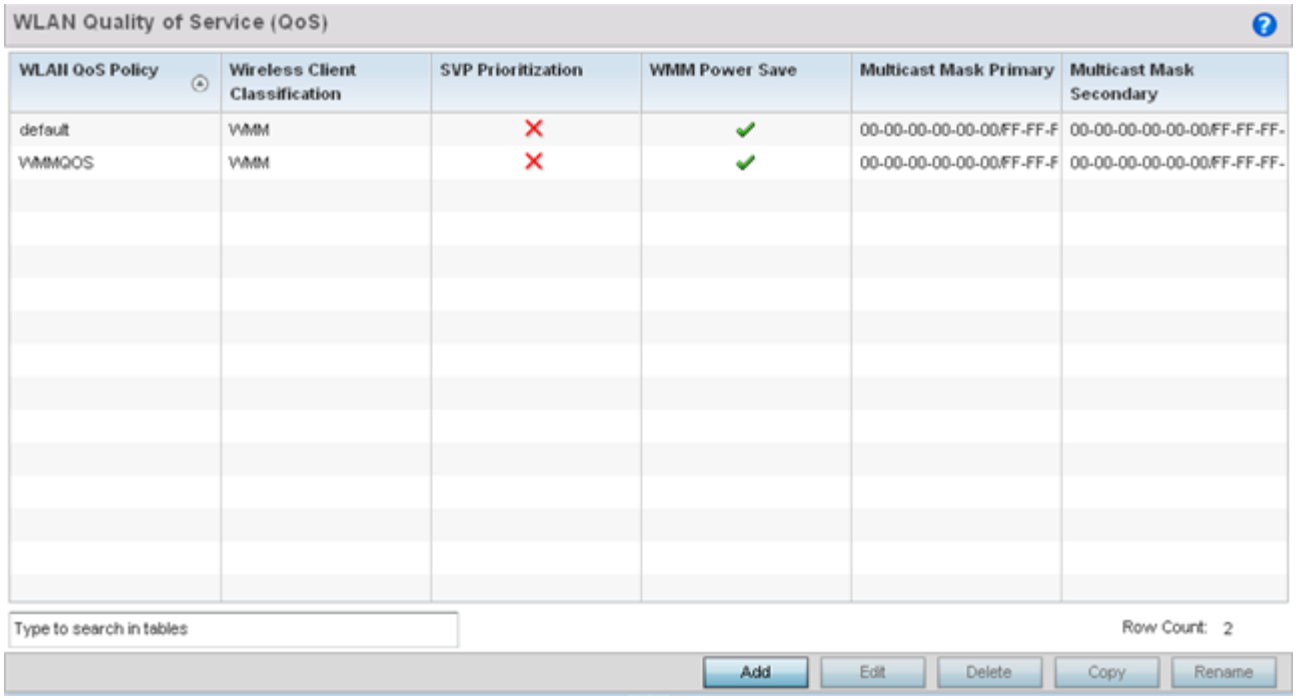



**Figure 301: WLAN QoS Screen**

2 Refer to the following read-only information on each listed QoS policy to determine whether a new policy needs to be created, an existing policy can be edited, or an existing policy can be used as is:

| | |
|---|---|
| WLAN QoS Policy | The name assigned to this WLAN QoS policy. The assigned policy name cannot be modified. |
| Wireless Client Classification | Each policy's Wireless Client Classification as defined for this WLAN's intended traffic. The Classification Categories are the different WLAN-WMM options available to a radio. Classification types include:<br>• **WMM** – Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). WMM classification is required to support the high throughput data rates required of 802.11n device support.<br>• **Voice**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.<br>• **Video** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.<br>• **Normal** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.<br>• **Low** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio. |
| SVP Prioritization | A green check mark defines the policy as having SVP *(Spectralink Voice Prioritization)* enabled to allow the wireless controller to identify and prioritize traffic from Spectralink/Polycomm phones using the SVP protocol. Phones using regular WMM and SIP are not impacted by SVP prioritization. A red "X" defines the QoS policy as not supporting SVP prioritization. |

| | |
|---|---|
| WMM Power Save | Enables support for the WMM based power-save mechanism, also known as U-APSD *(Unscheduled Automatic Power Save Delivery)*. This is primarily used by voice devices that are WMM capable. The default setting is enabled. |
| Multicast Mask Primary | The primary multicast mask defined for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling. |
| Multicast Mask Secondary | The secondary multicast mask defined for each listed QoS policy. |

3 Click **Add** to define a new WLAN QoS policy, or select an existing WLAN QoS policy and click **Edit** to modify its configuration. Existing QoS policies can be selected and deleted as needed.

A WLAN Quality of Service (QoS) policy screen displays for the new or selected WLAN. The screen displays the WMM tab by default, but additional tabs also display for WLAN and wireless client rate limit configurations. For more information, refer to the following:

- Configuring a WLAN's QoS WMM Settings on page 606
- Configuring a WLAN's QoS Rate Limit Settings on page 610
- Configuring Multimedia Optimizations on page 615

## Configuring a WLAN's QoS WMM Settings

Using WMM *(Wi-Fi Multimedia)*, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for both home networks and enterprises to decide which data streams are most important and assign them a higher traffic priority.

WMM's prioritization capabilities are based on the four access categories. The higher the access category, the higher the probability to transmit this kind of traffic over a controller, service platform or access point managed WLAN. Access categories were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled controllers, service platforms and access points can coexist with legacy devices (not WMM-enabled).

Packets not assigned to a specific access category are categorized by default as having best effort priority. Applications assign each data packet to a given access category packets are then added to one of four independent transmit queues (one per access category - voice, video, best effort or background) in the client. The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client(s) should be granted the TXOP *(opportunity to transmit)*. The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category.

- The minimum interframe space, or AIFSN *(Arbitrary Inter-Frame Space Number)*
- The contention window, sometimes referred to as the random backoff wait

Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest backoff values, they are more likely to get a TXOP.

After each collision the contention window is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the contention window is reset to its initial, AC dependant value. The AC with the lowest backoff value gets the TXOP.

To configure a WMM configuration for a WLAN:

1 Select **Configuration → Wireless → WLAN QoS Policy** to display existing QoS policies available to WLANs.

2 Click **Add** button to create a new QoS policy or **Edit** to modify the properties of an existing WLAN QoS policy.

The WMM tab displays by default.

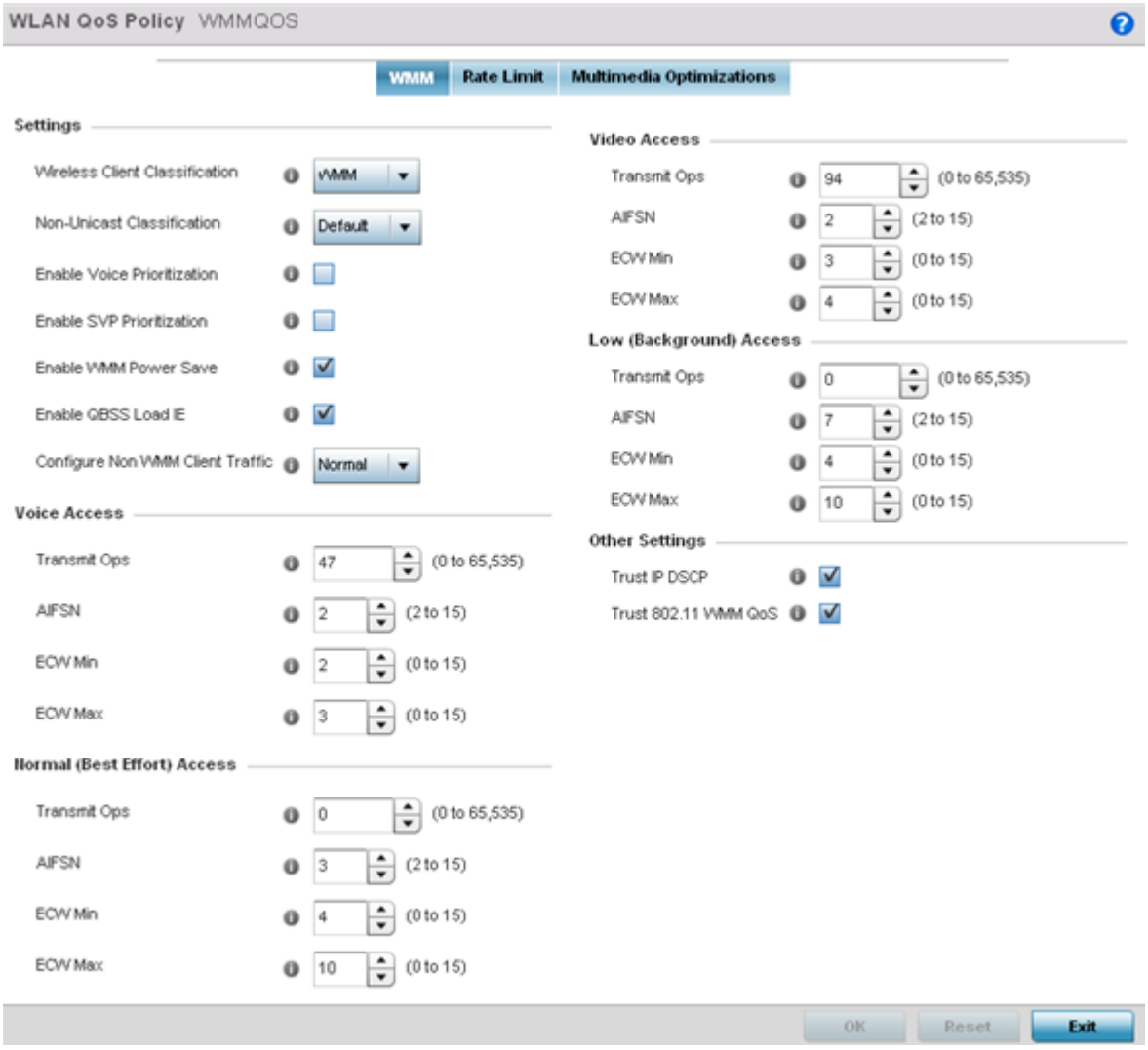



**Figure 302: WLAN QoS Policy Screen - WMM Tab**

3 Configure the following settings in respect to the WLAN's intended WMM radio traffic and user requirements:

| | |
|---|---|
| Wireless Client Classification | Use the drop-down menu to select the Wireless Client Classification for this WLAN's intended traffic type. The classification categories are the different WLAN-WMM options available to the radio. Classification types include:<br>• **WMM** – Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). WMM classification is required to support the high throughput data rates required of 802.11n device support. This is the default setting.<br>• **Voice**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.<br>• **Video** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.<br>• **Normal** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.<br>• **Low** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio. |
| Non-Unicast Classification | Use this drop-down menu to define how traffic matching multicast masks is classified relative to prioritization on the radio. Options include **Video**, **Voice**, **Normal**, **Low**, and **Default**. The default setting is **Default**. |
| Enable Voice Prioritization | Select this option if Voice traffic is prioritized on the WLAN. This gives priority to voice and voice management packets supported only on certain legacy VOIP phones. This feature is disabled by default. |
| Enable SVP Prioritization | Enabling SVP *(Spectralink Voice Prioritization)* allows the identification and prioritization of traffic from Spectralink/Polycomm phones. This gives priority to voice on certain legacy VOIP phones. If the wireless client classification is WMM, non WMM devices recognized as voice devices have their traffic transmitted at voice priority. Devices are classified as voice when they emit SIP, SCCP, or H323 traffic. Thus, selecting this option has no effect on devices supporting WMM. This feature is disabled by default. |
| Enable WMM Power Save | Enables support for the WMM based power-save mechanism, also known as U-APSD *(Unscheduled Automatic Power Save Delivery)*. This is primarily used by voice devices that are WMM capable. This feature is enabled by default. |
| Enable QBSS Load IE | Check this option to enable a QBSS *(QoS Basis Service Set)* IE *(information element)* in beacons and probe response packets advertised by access point radios. This feature is enabled by default. |
| Configure Non WMM Client Traffic | Use the drop-down menu to specify how non-WMM client traffic is classified on this access point WLAN if the Wireless Client Classification is set to WMM. Options include **Video**, **Voice**, **Normal**, and **Low**. The default setting is **Normal**. |

4 Set the following Voice Access settings for the WLAN's QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 47. |
| AIFSN | Set the current *Arbitrary Inter-frame Space Number* (AIFSN) between 2 and 15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2. |

| | |
|---|---|
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3. |

5 Set the following Video Access settings for the WLAN's QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default values is 94. |
| AIFSN | Set the current *Arbitrary Inter-frame Space Number* (AIFSN) between 2 and 15. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2. |
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 3. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 4. |

6 Set the following Normal (Best Effort) Access settings for the WLAN's QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 0. |
| AIFSN | Set the current AIFSN *(Arbitrary Inter-frame Space Number)* between 2 and 15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 3. |
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 4. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 10. |

7 Set the following Low (Background) Access settings for the WLAN's QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 0. |
| AIFSN | Set the current AIFSN between 2 and 15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 7. |

| | |
|---|---|
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 4. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 10. |

8 Set the following Other Settings for the WLAN's QoS policy:

| | |
|---|---|
| Trust IP DSCP | Select this option to trust (utilize) IP DSCP values for WLANs. The default value is enabled. |
| Trust 802.11 WMM QoS | Select this option to trust (utilize) 802.11 WMM QoS values for WLANs. The default value enabled. |

9 Click **OK** when completed to update this WLAN's QoS settings. Click **Reset** to revert the screen to its last saved configuration.

## Configuring a WLAN's QoS Rate Limit Settings

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. An administrator can set separate QoS rate limit configurations for data transmitted from the access point (upstream) and data transmitted from a WLAN's wireless clients back to their associated access point radios (downstream).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) will be dropped resulting in intermittent outages and performance problems.

To configure a QoS rate limit configuration for a WLAN and its connected clients:

1 Select **Configuration → Wireless → WLAN QoS Policy** to display existing QoS policies available to WLANs.
2 Click **Add** button to create a new QoS policy or **Edit** to modify the properties of an existing WLAN QoS policy.
3 Select the Rate Limit tab.

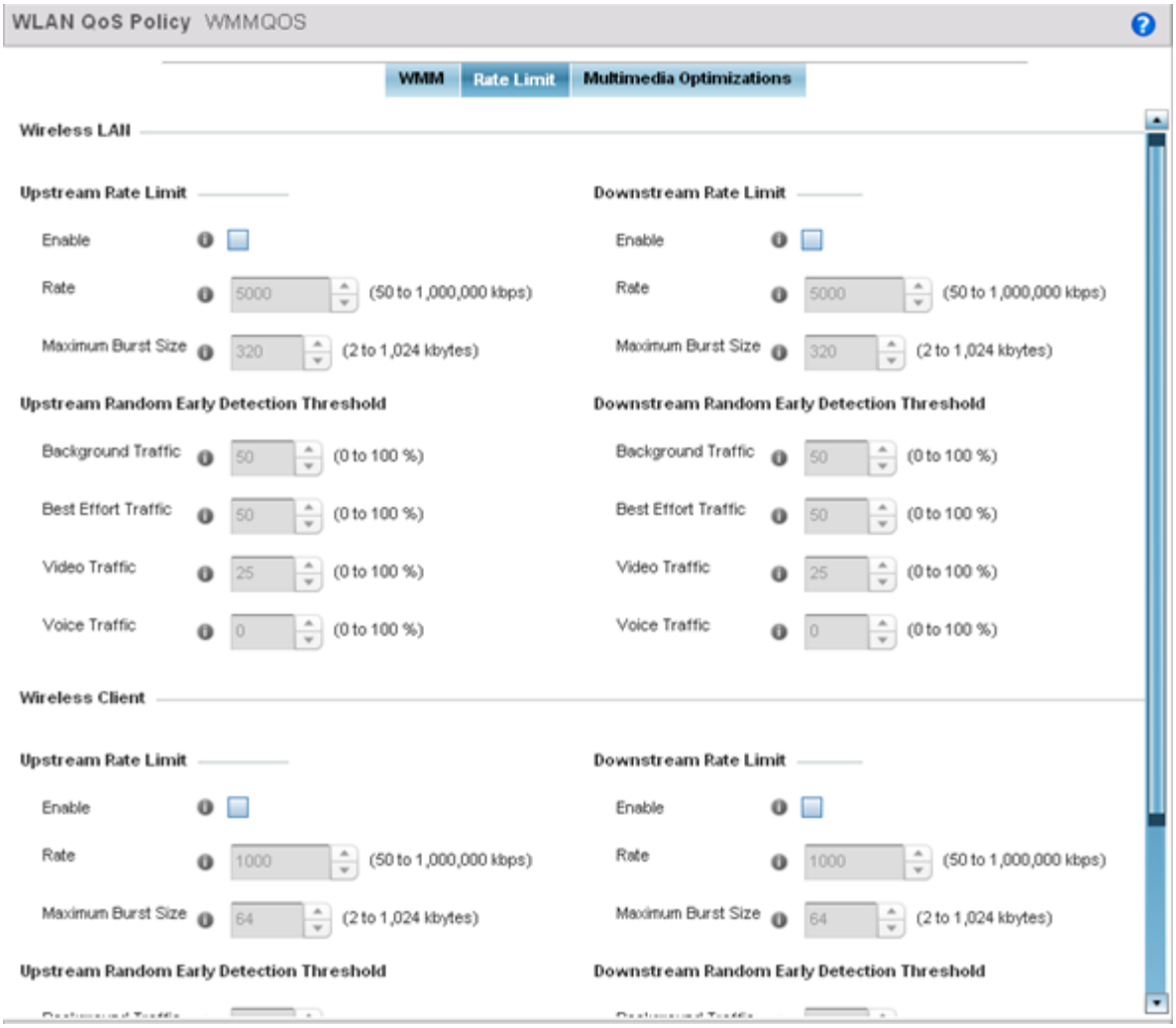



**Figure 303: WLAN QoS Policy Screen - Rate Limit Tab**

4 Configure the following parameters to define the **WLAN Upstream Rate Limit**.

| | |
|---|---|
| Enable | Select this option to enable rate limiting for data transmitted from access point radios to associated clients on this WLAN. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default. |
| Rate | Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps. |
| Maximum Burst Size | Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely an upstream packet transmission will result in congestion for the WLAN's client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes. |

5 Set the following **WLAN Upstream Random Early Detection Threshold** settings for each access category. An early random drop is done when a traffic stream falls below the set threshold.

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Video Traffic | Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the upstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. |

6 Configure the following parameters for the intended **WLAN Downstream Rate Limit**.

These values apply to traffic from wireless clients to associated access point radios.

| | |
|---|---|
| Enable | Select this option to enable rate limiting for data transmitted from access point radios to associated wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default. |
| Rate | Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps. |
| Maximum Burst Size | Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes. |

7 Set the following **WLAN Downstream Random Early Detection Threshold** settings for each access category. An early random drop is done when the amount of tokens for a traffic stream falls below the set threshold.

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Video Traffic | Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early om drops will occur. |

8 Configure the following parameters for the intended **Upstream Rate Limit** for wireless client rraffic:

| | |
|---|---|
| Enable | Select this option to enable rate limiting for data transmitted from access point radios to associated clients. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default. |
| Rate | Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps. |
| Maximum Burst Size | Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the wireless client. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes. |

9 Set the following **Upstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value, once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Video Traffic | Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.0% implies no early random drops will occur. |

10 Configure the following parameters for the **Downstream Rate Limit**.

These values apply to wireless client traffic.

| | |
|---|---|
| Enable | Select tis option to enable rate limiting for data transmitted from connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default. |
| Rate | Define a downstream rate limit between 50 - 1,000,000 kbps.This limit constitutes a threshold for the maximum the number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default rate is 1,000 kbytes. |
| Maximum Burst Size | Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for wireless client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes. |

11 Set the following **Downstream Random Early Detection Threshold** settings.

These setting apply to each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default is 50%. |
| Video Traffic | Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.0% means no early random drops will occur. |

12 Click **OK** when completed to update this WLAN's QoS rate limit settings. Click **Reset** to revert the screen to its last saved configuration.

## Configuring Multimedia Optimizations

To configure a QoS rate limit configuration for a WLAN:

1 Select **Configuration → Wireless → WLAN QoS Policy** to display existing QoS policies available to WLANs.

2 Click **Add** button to create a new QoS policy or **Edit** to modify the properties of an existing WLAN QoS policy.

3 Select the **Multimedia Optimizations** tab.

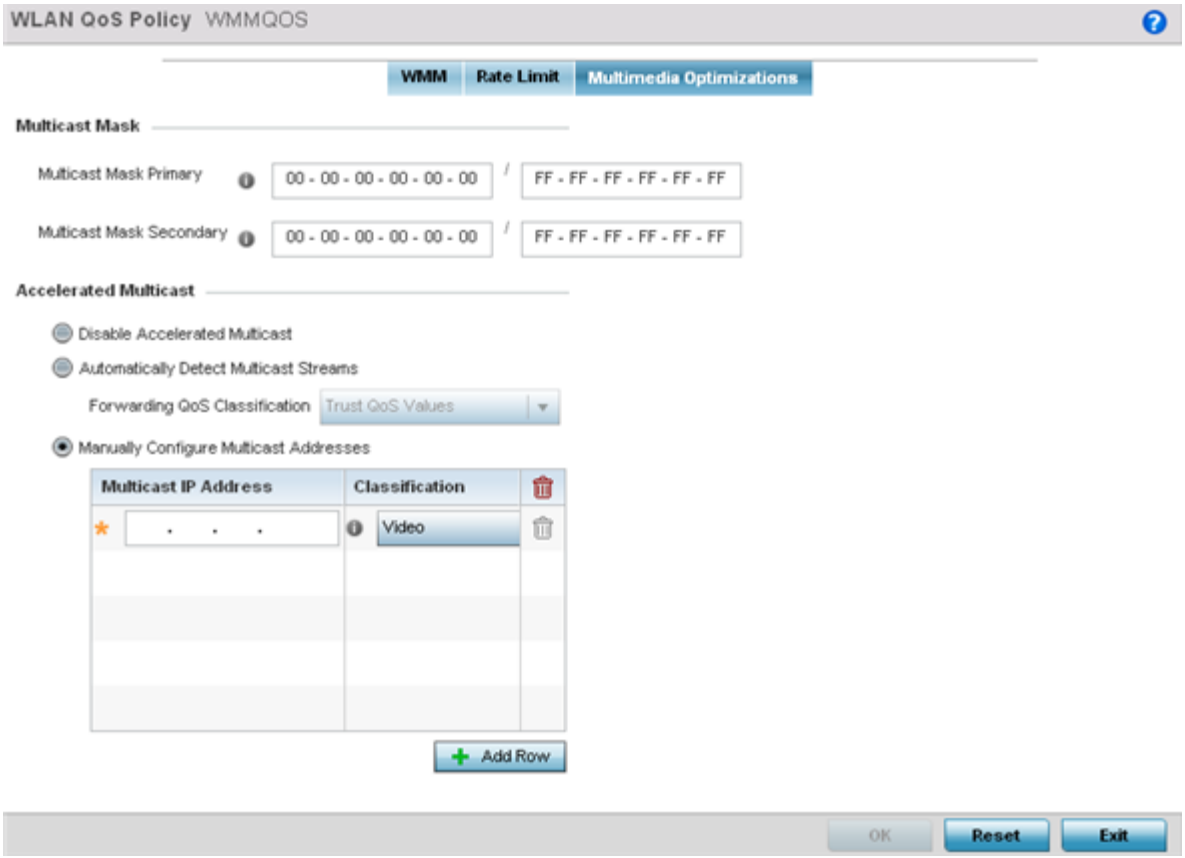



**Figure 304: WLAN QoS Policy Screen - Multimedia Optimizations Tab**

4 Configure the following parameters for to the **Multicast Mask**:

| | |
|---|---|
| Multicast Mask Primary | Configure the primary multicast mask defined for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling. |
| Multicast Mask Secondary | Set a secondary multicast mask for the WLAN QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling. |

5 Set the following **Accelerated Multicast** settings:

| | |
|---|---|
| Disable Multicast Streaming | Select this option to disable all accelerated multicast streaming on the WLAN. |
| Automatically Detect Multicast Streams | Select this option to have multicast packets converted to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are converted to unicast. When the stream is converted and queued for transmission, a number of classification mechanisms can be applied to the stream, and the administrator can select the desired classification type. Use the **Forwarding QoS Classification** drop-down list to select the classification to use. |
| Manually Configure Multicast Addresses | Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches. |

6 Click **OK** when completed to update this WLAN's multimedia optimization settings. Click **Reset** to revert the screen to its last saved configuration.

### WLAN QoS Deployment Considerations

Before defining a QoS configuration on a controller, service platform or access point managed WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WLAN QoS configurations differ significantly from QoS policies configured for associated radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients the radios support.
- Enabling WMM support on a WLAN only advertises WMM capability to wireless clients. The wireless clients must also support WMM and use the parameters correctly while accessing the wireless network to truly benefit.
- Rate limiting is disabled by default on WLANs. To enable rate limiting, a threshold must be defined for WLAN.
- Before enabling rate limiting on a WLAN, a baseline for each traffic type should be performed. Once a baseline has been determined, a minimum 10% margin should be added to allow for traffic bursts.
- The bandwidth required for real-time applications such as voice and video are very fairly easy to calculate because the bandwidth requirements are consistent and can be realistically trended over time. Applications such as web, database, and email are harder to estimate because bandwidth usage varies depending on how the applications are used.

## Radio QoS Policies

Without a dedicated QoS policy, any wireless network operates on a best-effort delivery basis, meaning all traffic has equal priority and equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a QoS policy for a radio, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customizations best suited to each QoS policy's intended wireless client base.

WiNG managed controllers and their associated access point radios and wireless clients support several *Quality of Service* (QoS) techniques enabling real-time applications (such as voice and video) to coexist

with lower priority background applications (such as web, email, and file transfers). A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize the network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent the ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy.

In a wireless network, wireless clients supporting low and high priority traffic contend with one another for access and data resources. The IEEE 802.11e amendment has defined *Enhanced Distributed Channel Access* (EDCA) mechanisms stating high priority traffic can access the network sooner then lower priority traffic. The EDCA defines four traffic classes (or access categories): voice (highest), video (next highest), best effort, and background (lowest). The EDCA has defined a time interval for each traffic class, known as the *Transmit Opportunity* (TXOP). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported by the controller or service platform, their associated access points and connected radios.

IEEE 802.11e includes an advanced power saving technique called *Unscheduled Automatic Power Save Delivery* (U-APSD) that provides a mechanism for wireless clients to retrieve packets buffered by an access point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an access point. U-APSD also allows access points to deliver buffered data frames as *bursts*, without backing-off between data frames. These improvements are useful for voice clients, as they provide improved battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save*(WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. An access point managed wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must be also able to support WMM and use the values correctly while accessing the WLAN.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters apply to both connected access point radios and their wireless clients. Parameters that affect access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

Access points support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. An access point allows flexible WLAN mapping with a static WMM access control value. When enabled on a WLAN, traffic forwarded from to a client is prioritized and forwarded based on the WLAN's WMM access control setting.

Note

Statically setting a WLAN WMM access category value prioritizes traffic to the client, but does not prioritize traffic from the client.

Wireless network administrators can also assign weights to each WLAN in relation to user priority levels. The lower the weight, the lower the priority. Use a weighted round robin technique to achieve different QoS levels across WLANs.

You can rate-limit bandwidth for WLAN sessions. This form of per-user rate limiting enables administrators to define uplink and downlink bandwidth limits for users and clients. This sets the level of traffic a user or client can forward and receive over the WLAN. If the user or client exceeds the limit, excessive traffic is dropped.

Rate limits can be applied externally from a RADIUS server using Vendor Specific Attributes (VSAs). Rate limits can be applied to users authenticating using 802.1X, captive portal authentication and devices using MAC authentication.

## Configuring a Radio QoS Policy

To configure an access point radio's QoS policy:

1 Select **Configuration** > **Wireless** > **Radio QoS Policy** to display existing radio QoS policies.

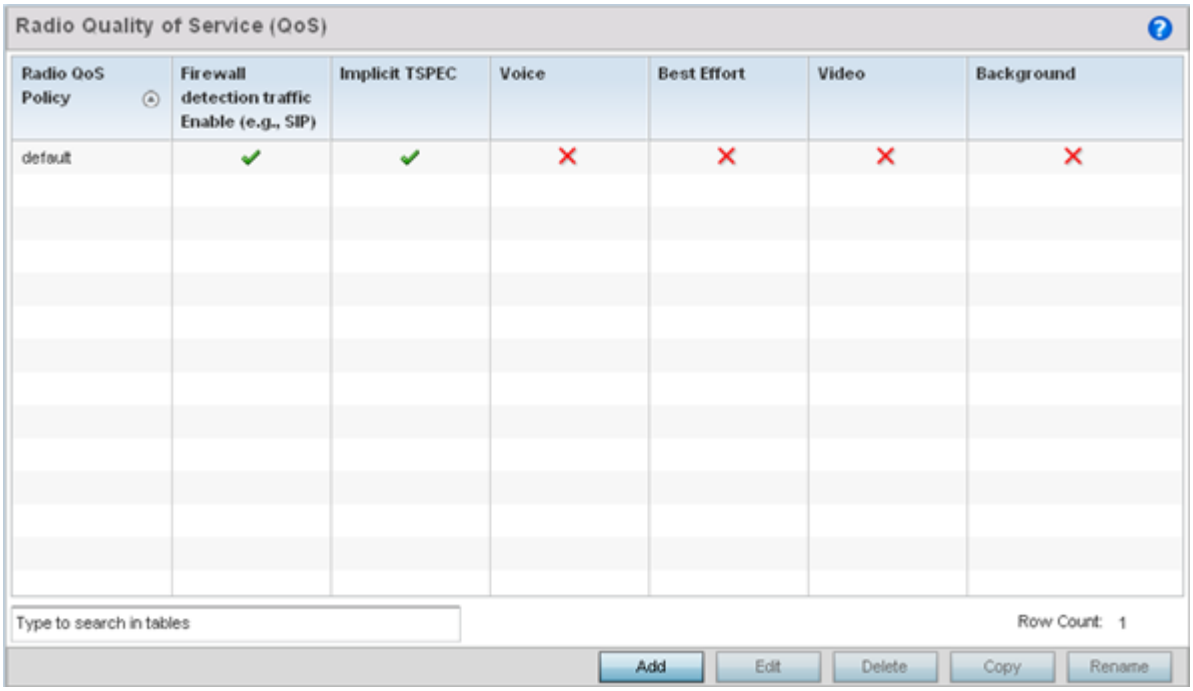



**Figure 305: Radio QoS Policy Screen**

The Radio QoS Policy screen lists those radio QoS policies created thus far. Any of these policies can be selected and applied.

2 Refer to the following information listed for each existing radio QoS policy:

| | |
|---|---|
| Radio QoS Policy | Displays the name of each radio QoS policy. This is the name set for each listed policy when it was created and cannot be modified as part of the policy edit process. |
| Firewall detection traffic Enable (e.g., SIP) | A green check mark defines the policy as applying radio QoS settings to traffic detected by the Firewall. A red X defines the policy as having Firewall detection disabled. When enabled, the Firewall simulates the reception of frames for voice traffic when the voice traffic was originated via SIP or SCCP control traffic. If a client exceeds configured values, the call is stopped and/or received voice frames are forwarded at the next non admission controlled traffic class priority. This applies to clients that do not send TPSEC frames only. |
| Implicit TPSEC | A green check mark defines the policy as requiring wireless clients to send their traffic specifications before they can transmit or receive data. If enabled, this setting applies to just this radio's QoS policy. When enabled, the Access Point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If the client sends more traffic than has been configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TPSEC frames only. |
| Voice | A green check mark indicates that Voice prioritization QoS is enabled on the radio. A red X indicates that **Voice** prioritization QoS is disabled on the radio. |
| Best Effort | A green check mark indicates that Best Effort QoS is enabled on the radio. A red X indicates that **Best Effort** QoS is disabled on the radio. |
| Video | A green check mark indicates that Video prioritization QoS is enabled on the radio. A red X indicates that **Video** prioritization QoS is disabled on the radio. |
| Background | A green check mark indicates that Background prioritization QoS is enabled on the radio. A red X indicates that **Background** prioritization QoS is disabled on the radio. |

3 Click **Add** to create a new radio QoS policy, or select an existing policy and click **Edit** to modify its configuration.

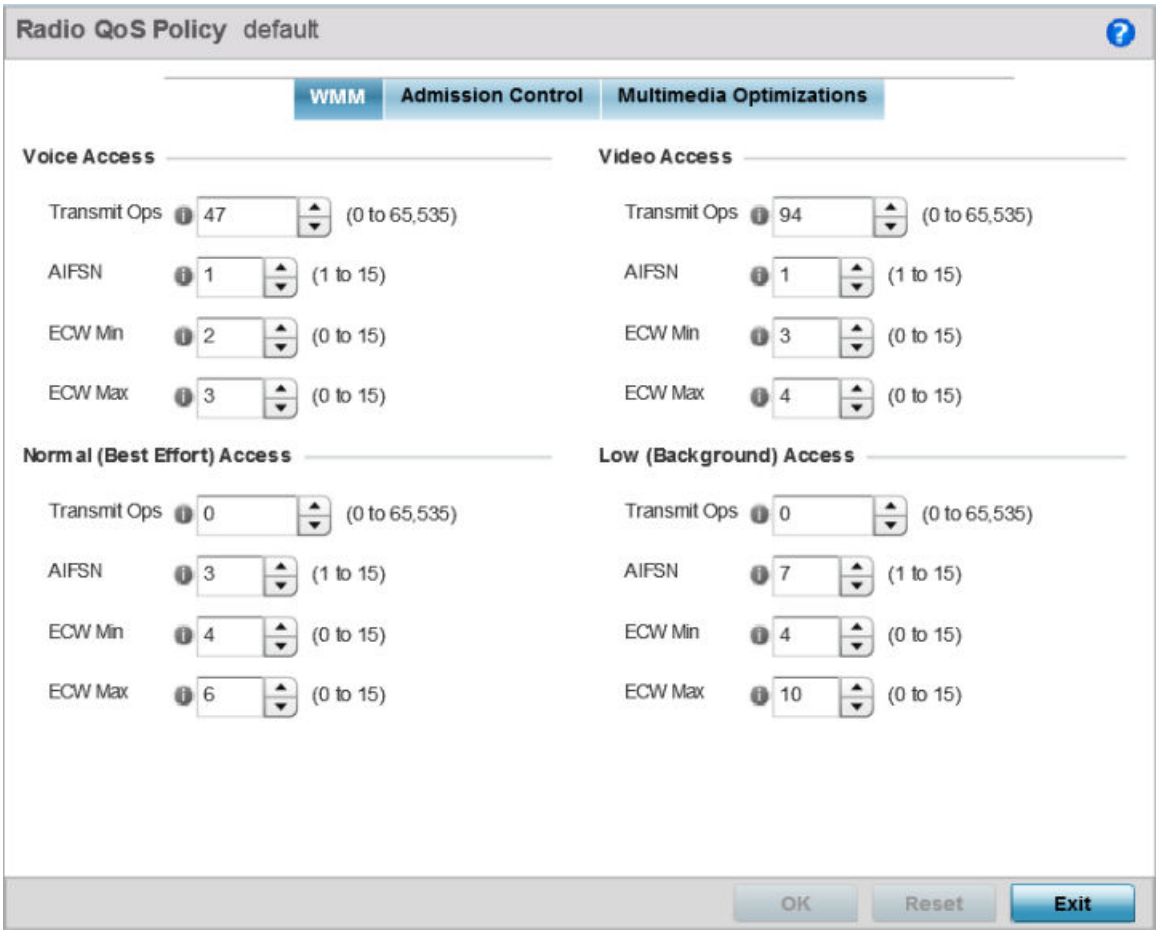



**Figure 306: Radio QoS Policy WMM Screen**

The Radio QoS Policy screen displays the WMM tab by default. Use the WMM tab to define the access category configuration (CWMin, CWMax, AIFSN and TXOP values) in respect to the type of wireless data planned for this new or updated radio QoS policy.

4 Set the following **Voice Access** settings for the radio QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. When resources are shared between a Voice over IP (VoIP) call and a low priority file transfer, bandwidth is normally exploited by the file transfer, thus reducing call quality or even causing the call to disconnect. With voice QoS, a VoIP call (a realtime session), receives priority, maintaining a high level of voice quality. For higher-priority traffic categories (like voice), the **`Transmit Ops`** value should be set to a low number. The default value is 47. |
| AIFSN | Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1. |

| | |
|---|---|
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3. |

5 Set the following **Normal (Best Effort) Access** settings for the radio QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0. |
| AIFSN | Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 3. |
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 4. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 6. |

6 Set the following **Video Access** settings for the radio QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 94. |
| AIFSN | Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1. |
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 4. |

7 Set the following **Low (Background) Access** settings for the radio QoS policy:

| | |
|---|---|
| Transmit Ops | Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0. |
| AIFSN | Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 7. |

| | |
|---|---|
| ECW Min | The **ECW Min** is combined with the **ECW Max** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 4. |
| ECW Max | The **ECW Max** is combined with the **ECW Min** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 10. |

8 Click **OK** when completed to update the radio QOS settings for this policy.

Click **Reset** to revert the WMM screen to its last saved configuration.

9 Select the Admission Control tab to configure an admission control configuration for the selected radio QoS policy.

Admission control requires clients send their traffic specifications (TSPEC) to a controller or service platform managed Access Point before they can transmit or receive data.

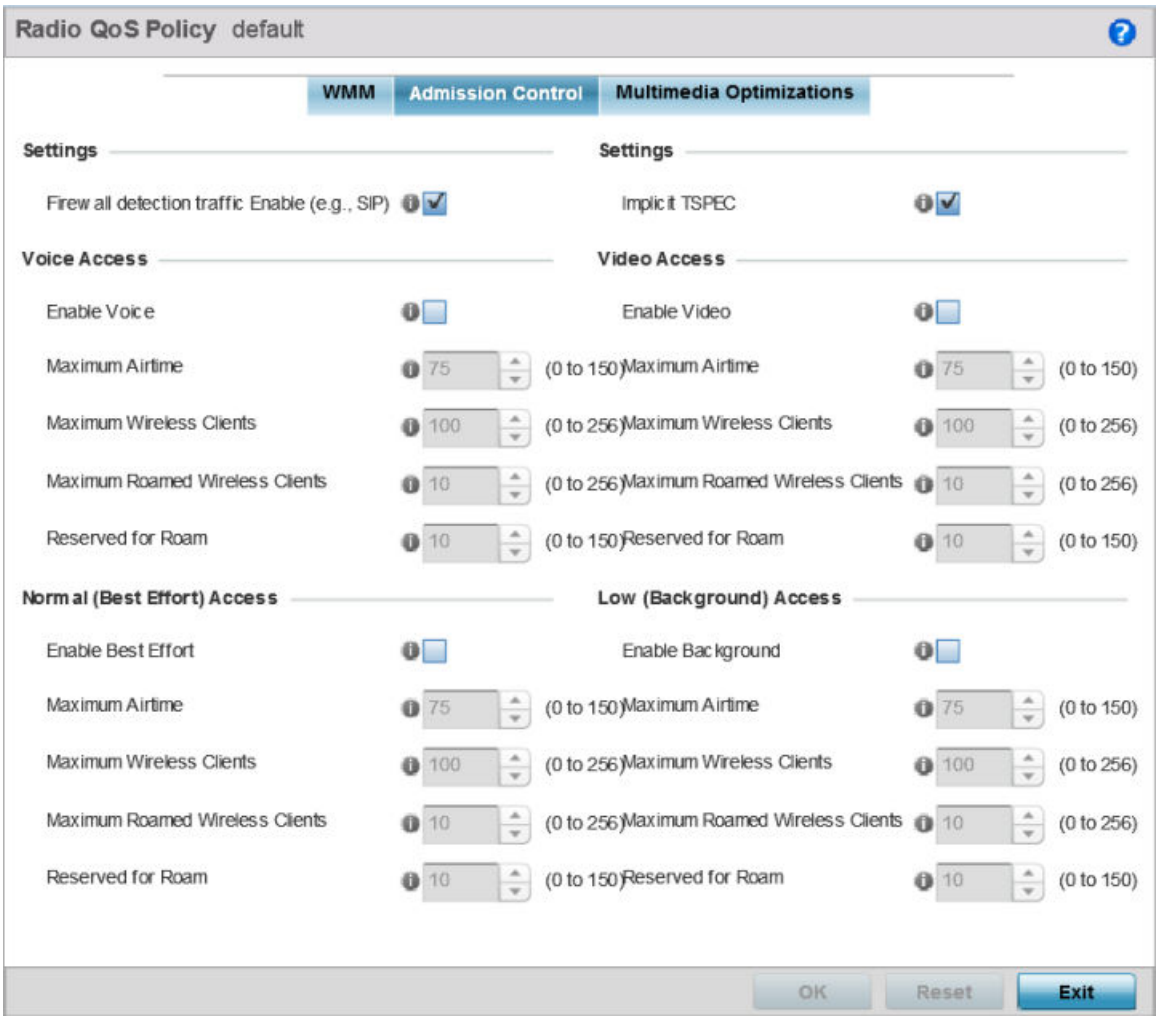



**Figure 307: Radio QoS Policy Admission Control Screen**

The name of the radio QoS policy for which the admission control settings apply displays in the banner of the QoS Policy screen.

10 Select the **Firewall detection traffic Enable (e.g, SIP)** check box to force admission control to traffic whose access category is detected by the firewall.

This feature is enabled by default.

11 Select the **Implicit TSPEC** check box to require wireless clients to send their traffic specifications to a controller or service platform managed access point before they can transmit or receive data.

If enabled, this setting applies to the QoS policy for this radio only. This feature is enabled by default.

12 Set the following **Voice Access** admission control settings for this radio QoS policy:

| | |
|---|---|
| Enable Voice | Select the check box to enable admission control for this policy's voice traffic. Only voice traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). |
| Maximum Airtime | Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value ensures the radio's bandwidth is available for high bandwidth voice traffic (if anticipated on the wireless medium) or other access category traffic if voice support is not prioritized. Voice traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support voice. The default value is 75%. |
| Maximum Wireless Clients | Set the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. Consider setting this value proportionally to the number of other QoS policies supporting the voice access category, as wireless clients supporting voice use a greater proportion of resources than lower bandwidth traffic (like low and best effort categories). The default value is 100 clients. |
| Maximum Roamed Wireless Clients | Set the number of voice supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients. |
| Reserved for Roam | Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%. |

13 Set the following **Normal (Best Effort) Access** admission control settings for this radio QoS policy:

| | |
|---|---|
| Enable Best Effort | Select the check box to enable admission control for this policy's normal traffic. Only normal traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). |
| Maximum Airtime | Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal best effort client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for lower bandwidth normal traffic (if anticipated to proliferate the wireless medium). Normal background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for best effort data support. The default value is 75%. |
| Maximum Wireless Clients | Set the number of wireless clients supporting best effort traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients. |

| | |
|---|---|
| Maximum Roamed Wireless Clients | Set the number of normal best effort supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients. |
| Reserved for Roam | Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal best effort supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%. |

14 Set the following **Video Access** admission control settings for this radio QoS policy:

| | |
|---|---|
| Enable Video | Select the check box to enable admission control for this policy's video traffic. Only video traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default. |
| Maximum Airtime | Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for high bandwidth video traffic (if anticipated on the wireless medium) or other access category traffic if video support is not prioritized. Video traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support video. The default value is 75%. |
| Maximum Wireless Clients | Set the number of wireless clients supporting video traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients. |
| Maximum Roamed Wireless Clients | Set the number of video supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients. |
| Reserved for Roam | Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%. |

15 Set the following **Low (Background) Access** admission control settings for this radio QoS policy:

| | |
|---|---|
| Enable Background | Select the check box to enable admission control for this policy's lower priority background traffic. Only low background traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). |
| Maximum Airtime | Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for low background client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for lower bandwidth normal traffic (if anticipated to proliferate the wireless medium). Background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for background data support. The default value is 75%. |
| Maximum Wireless Clients | Set the number of low and background supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients. |

| | |
|---|---|
| Maximum Roamed Wireless Clients | Set the number of low and best effort supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients. |
| Reserved for Roam | Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal background supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%. |

16 Select the Multimedia Optimizations tab to set the advanced multimedia QoS and Smart Aggregation configuration for selected radio QoS policy.

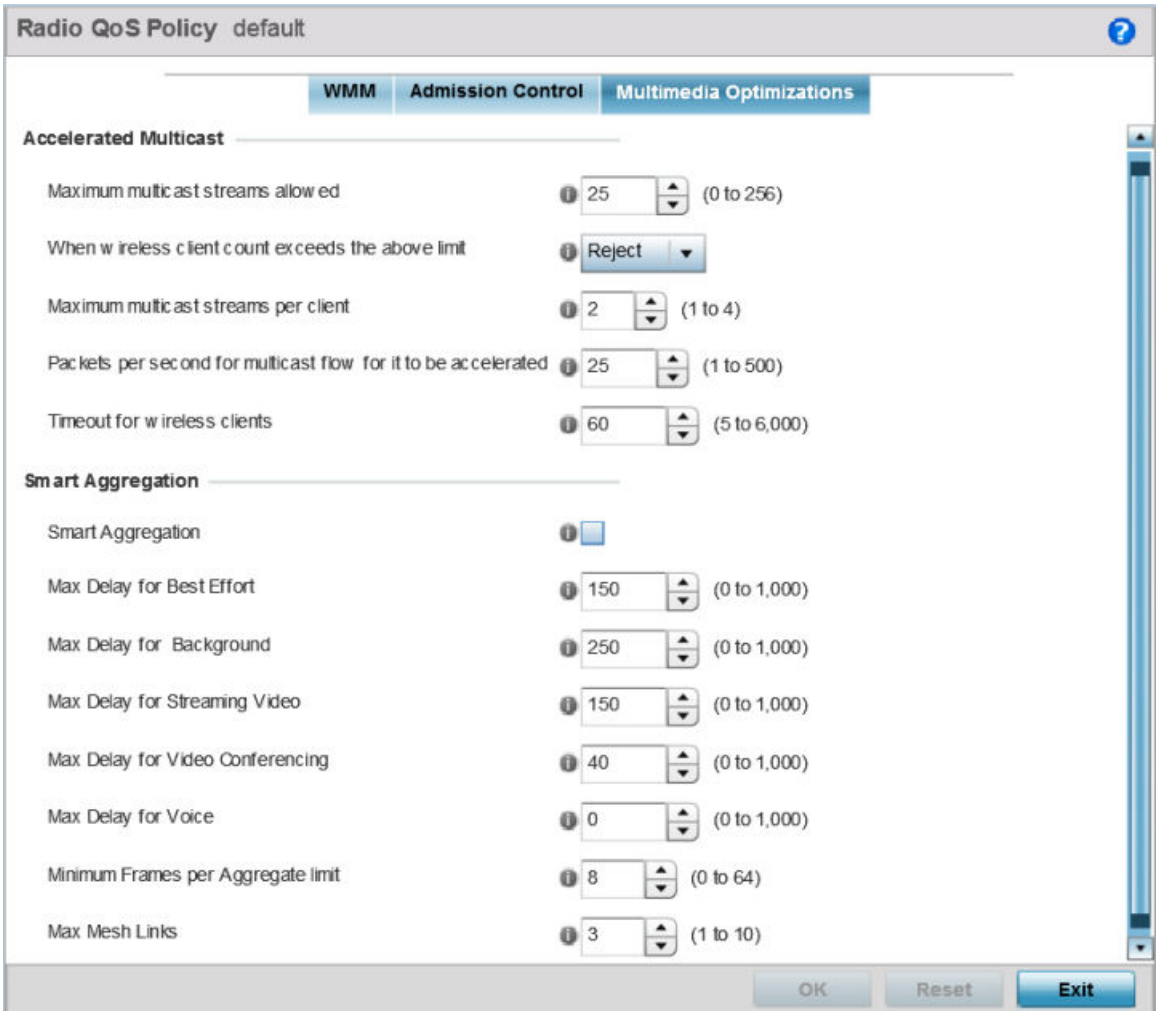



**Figure 308: Radio QoS Policy Multimedia Optimizations Screen**

17 Set the following **Accelerated Multicast** settings for this radio QoS policy:

| | |
|---|---|
| Maximum multicast streams allowed | Specify the maximum number of multicast streams (between 0 and 256) permitted to use accelerated multicast. The default value is 25. |
| When wireless client count exceeds the above limit | When the wireless client count using accelerated multicast exceeds the maximum number, set the radio to either **`Reject`** new wireless clients or **`Revert`** existing clients to a non-accelerated state. |

| | |
|---|---|
| Maximum multicast streams per client | Specify the maximum number of multicast streams (between 1 and 4) wireless clients can use. The default value is 2. |
| Packets per second for multicast flow for it to be accelerated | Specify the threshold of multicast packets per second (between 1 and 500) that triggers acceleration for wireless clients. The default value is 25. |
| Timeout for wireless clients | Specify a timeout value in seconds (between 5 and 6,000) for wireless clients to revert to a non-accelerated state. The default value is 60. |

18 Define the following **Smart Aggregation** settings:

Smart Aggregation enhances frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In a frame's typical aggregation, an aggregated frame is sent when it meets one of these conditions:

- A preconfigured number of aggregated frames is reached
- An administrator defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received
- An administrator defined interval has elapsed since the last frame (not necessarily the final frame) of a set of frames to be aggregated was received

With this enhancement, an aggregation delay is set uniquely for each traffic class. For example, voice traffic might not be aggregated, but sent immediately. Whereas, background data traffic is set a delay for aggregating frames, and these aggregated frames are sent.

| | |
|---|---|
| Smart Aggregation | Select to enable smart aggregation and dynamically define when an aggregated frame is transmitted. Smart aggregation is disabled by default. |
| Max Delay for Best Effort | Set the maximum time (in milliseconds) to delay best effort traffic. The default setting is 150 milliseconds. |
| Max Delay for Background | Set the maximum time (in milliseconds) to delay background traffic. The default setting is 250 milliseconds. |
| Max Delay for Streaming Video | Set the maximum time (in milliseconds) to delay streaming video traffic. The default setting is 150 milliseconds. |
| Max Delay for Video Conferencing | Set the maximum time (in milliseconds) to delay video conferencing traffic. The default setting is 40 milliseconds. |
| Max Delay for Voice | Set the maximum time (in milliseconds) to delay voice traffic. The default setting is 0 milliseconds. |
| Minimum frames per Aggregate limit | Set the minimum number of frames to aggregate in a frame before it is transmitted. The default setting is 8 frames. |
| Max Mesh Links | Set the maximum number of mesh hops for smart aggregation. The default setting is 3. |

19 Click **OK** when completed to update the radio QOS settings for this policy.

Click **Reset** to revert to the last saved configuration.

## Radio QoS Configuration and Deployment Considerations

Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- To support QoS, each multimedia application, wireless client and WLAN is required to support WMM.
- WMM enabled clients can coexist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a best effort access category.
- Use default WMM values for all deployments. Changing these values can lead to unexpected traffic blockages, and these blockages might be difficult to diagnose.
- Overloading an access point radio with too much high priority traffic (especially voice) degrades overall service quality for all of its users.
- TSPEC admission control is available only with newer voice over WLAN phones. Many legacy voice devices do not support TPSEC or even support WMM traffic prioritization.

## Association ACL

An association ACL is a policy-based ACL that either allows or denies clients from connecting to a controller, service platform or access point managed WLAN. An association ACL affords a system administrator the ability to restrict access by specifying a client MAC address or range of addresses to either include or exclude from WLAN connectivity.

Association ACLs are applied to WLANs as an additional access control mechanism. They can be applied to WLANs from within a WLAN Policy's Advanced Configuration screen. For more information on applying an existing association ACL to a WLAN, see Configuring Advanced WLAN Settings on page 596.

Each supported access point model supports 32 association ACLs.

To define an association ACL deployable with a WLAN:

1 Select **Configuration → Wireless → Association ACL** to display existing association ACLs.

Any of the policies listed in the Association Access Control List (ACL) screen can be selected and applied.

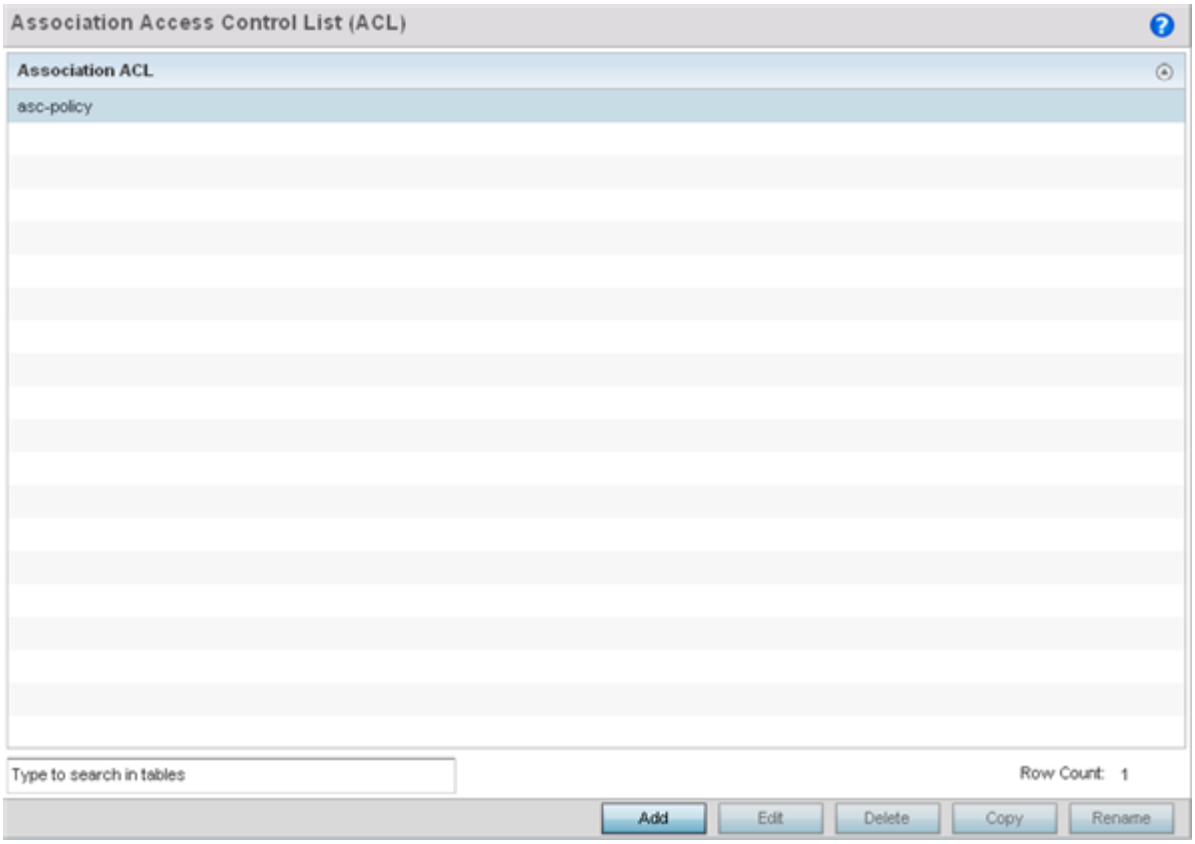



**Figure 309: Association Access Control List (ACL) Screen**

2 Review existing Association ACLs to determine if a new policy warrants creation or an existing policy warrants modification or deletion.

3 Select **Add** to define a new ACL configuration, **Edit** to modify an existing ACL configuration, or **Delete** to remove one. Select **Copy** to make a copy of an existing ACL for further modifications. Select **Rename** to rename an existing ACL.

An Association ACL screen displays for defining a new ACL or modifying a selected ACL.

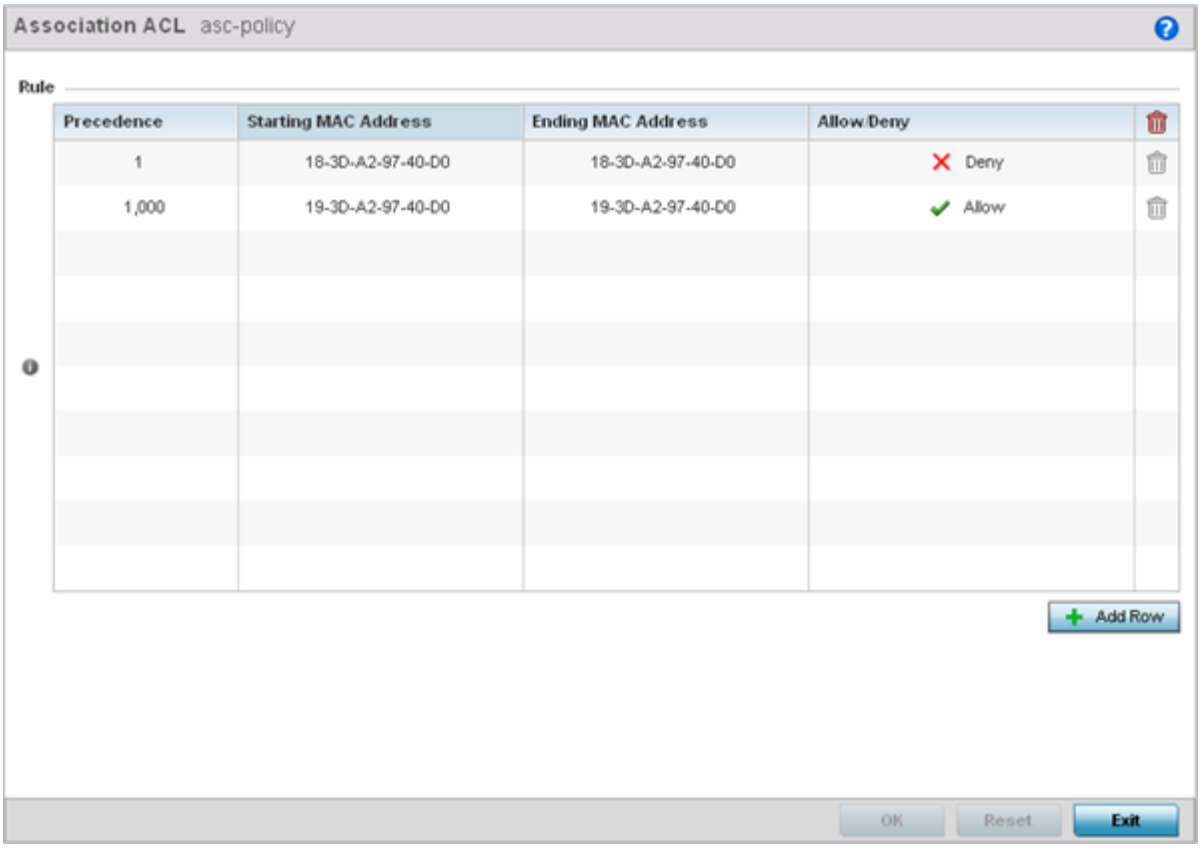



**Figure 310: Association ACL Screen**

4 Select the **+ Add Row** button to add an association ACL template.

5 Set the following parameters to create or modify the association ACL:

| | |
|---|---|
| Association ACL | If you are creating an new Association ACL, provide a name specific to its function. Avoid naming it after the WLAN it supports. The name cannot exceed 32 characters. |
| Precedence | The rules within a WLAN's ACL are applied to packets based on precedence. Every rule has a unique sequential precedence value you define. You cannot add two rules with the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added. |
| Starting MAC Address | Provide a starting client MAC address for non unicast and multicast packet transmissions. |
| Ending MAC Address | Provide an ending client MAC address for non unicast and multicast packet transmissions. |
| Allow/Deny | Use the drop-down menu to **`Allow`** or **`Deny`** access if a MAC address matches this rule. |

6 Select the **+ Add Row** button to add MAC address ranges and allow/deny designations.

7 Click **OK** to update the association ACL settings. Click **Reset** to revert to the last saved configuration.

### Association ACL Deployment Considerations

Before defining an association ACL configuration and applying it to a controller, service platform or access point managed WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Use the Association ACL screen strategically to name and configure ACL policies meeting the requirements of the particular WLANs to which they apply. Be careful, however, not to name ACLs after specific WLANs, because individual ACL policies can be used by more than one WLAN.
- You cannot apply more than one MAC based ACL to a Layer 2 interface. If a MAC ACL is already configured on a Layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

## Smart RF Policies

*Self Monitoring At Run Time RF Management* (Smart RF) is an innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization radio performance improvements.

A Smart RF policy can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power for each managed radio.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs through periodic re-calibration of the network. Recalibration can be initiated manually or can be automatically scheduled to ensure the RF configuration is optimized to factor for RF environment changes (such as new sources of interference, or neighboring access points).

Note

Unlike a controller or service platform, an access point utilizes a single Smart RF configuration it can use with other access points of the same model. However, the Smart RF policy needs to be activated from any one of the Smart RF screens. Numerous Smart RF policies cannot be defined on behalf of the access point.

Smart RF also provides self-healing functions by monitoring the network in real-time and provides automatic mitigation from potentially problematic events such as radio interference, non-WiFi interference (noise), external WiFi interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual reconfiguration to resolve.

If a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.
- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks a channel specified in the Smart RF policy.
- If no Smart RF policy is mapped, the radio selects a random channel.

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access points detects radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using a `no dfs-rehome` command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

**Note**

RF planning must be performed to ensure overlapping coverage exists at a deployment site for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

**Caution**

The access point's Smart RF feature is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections and communication disruptions.

## Configuring Smart RF Basic Settings

To define a Smart RF policy:

1 Select **Configuration** > **Wireless** > **Smart RF**.

The Basic Configuration screen displays by default.

2 Select the **Activate SMART RF Policy** check box to enable the parameters on the screen for configuration.

The configuration cannot be applied to the access point profile unless this setting is selected and remains enabled.

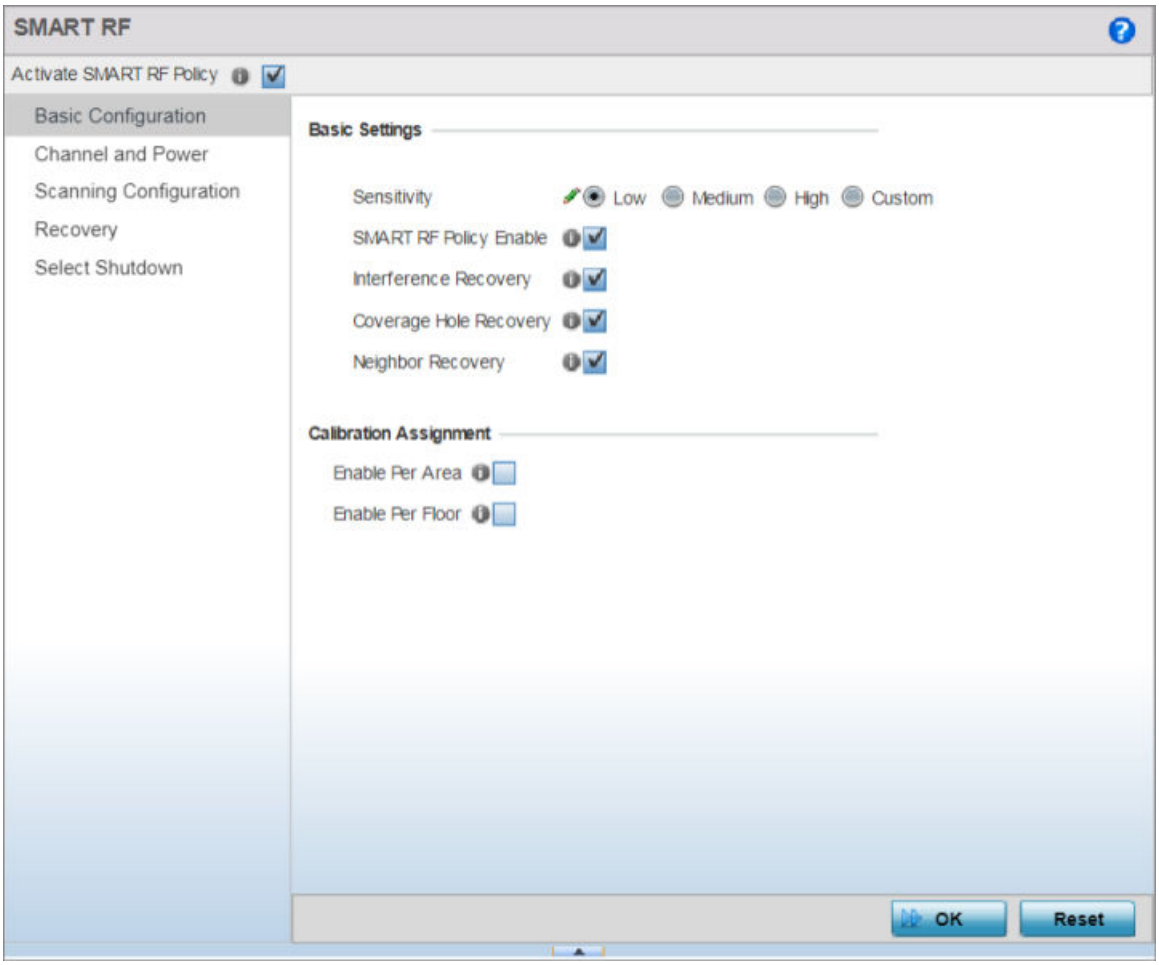



**Figure 311: SMART RF - Basic Configuration Screen**

3 Refer to the **Basic Settings** field to enable a Smart RF policy and define its sensitivity and detector status.

| | |
|---|---|
| Sensitivity | Select a radio button corresponding to the desired Smart RF sensitivity. Options include **Low**, **Medium**, **High**, and **Custom**. **Medium** is the default setting. |
| Smart RF Policy Enable | Select this option to enable Smart RF for immediate inclusion within an RF Domain. Smart RF is enabled by default. |

| | |
|---|---|
| Interference Recovery | Select this option to enable compensations from neighboring radios when radio interference is detected. When interference is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client (as seen by the access point radio). If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. This option is enabled by default.<br>Select this option to enable Interference Recovery from neighboring radios and other sources of WiFi and non-WiFi interference when excess noise and interference is detected within the Smart RF supported radio coverage area. Smart RF provides mitigation from interference sources by monitoring the noise levels and other RF parameters on an Access Point radio's current channel. When a noise threshold is exceeded, Smart RF can select an alternative channel with less interference. To avoid channel flapping, a hold timer is defined which disables interference avoidance for a specific period of time upon detection. Interference Recovery is enabled by default. |
| Coverage Hole Recovery | Select this option to enable coverage compensation from neighboring radios when a radio coverage hole is detected within the Smart RF supported radio coverage area. When a coverage hole is detected, Smart RF first determines the power increase needed based on the signal-to-noise ratio for a client as seen by the access point radio. If a client's signal-to-noise value is above the threshold, the transmit power is increased until the signal-to-noise rate falls below the threshold. This option is enabled by default. |
| Neighbor Recovery | Select this option to enable automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. This option is enabled by default. |

4 Refer to the **Calibration Assignment** field to define whether Smart RF Calibration and radio grouping is conducted by area or floor.

Both options are disabled by default.

5 Click **OK** to update the Smart RF basic settings for this policy.

Click **Reset** to revert to the last saved configuration.

The Smart RF policy can be invoked at any point in the configuration process by selecting **Activate SMART RF Policy** from the upper, left-hand portion of the access point user interface.

## Configuring Smart RF Channel & Power Settings

To configure Smart RF Channel and Power settings:

1 Select **Channel and Power**.

Use the Channel and Power screen to refine Smart RF power settings over both the 5.0 GHz and 2.4 GHz radio bands and select channel settings in respect to the access point's channel usage.

Note
The **Power Settings** and **Channel Settings** parameters are enabled only when **`Custom`** is selected as the **Sensitivity** setting from the Basic Configuration screen.

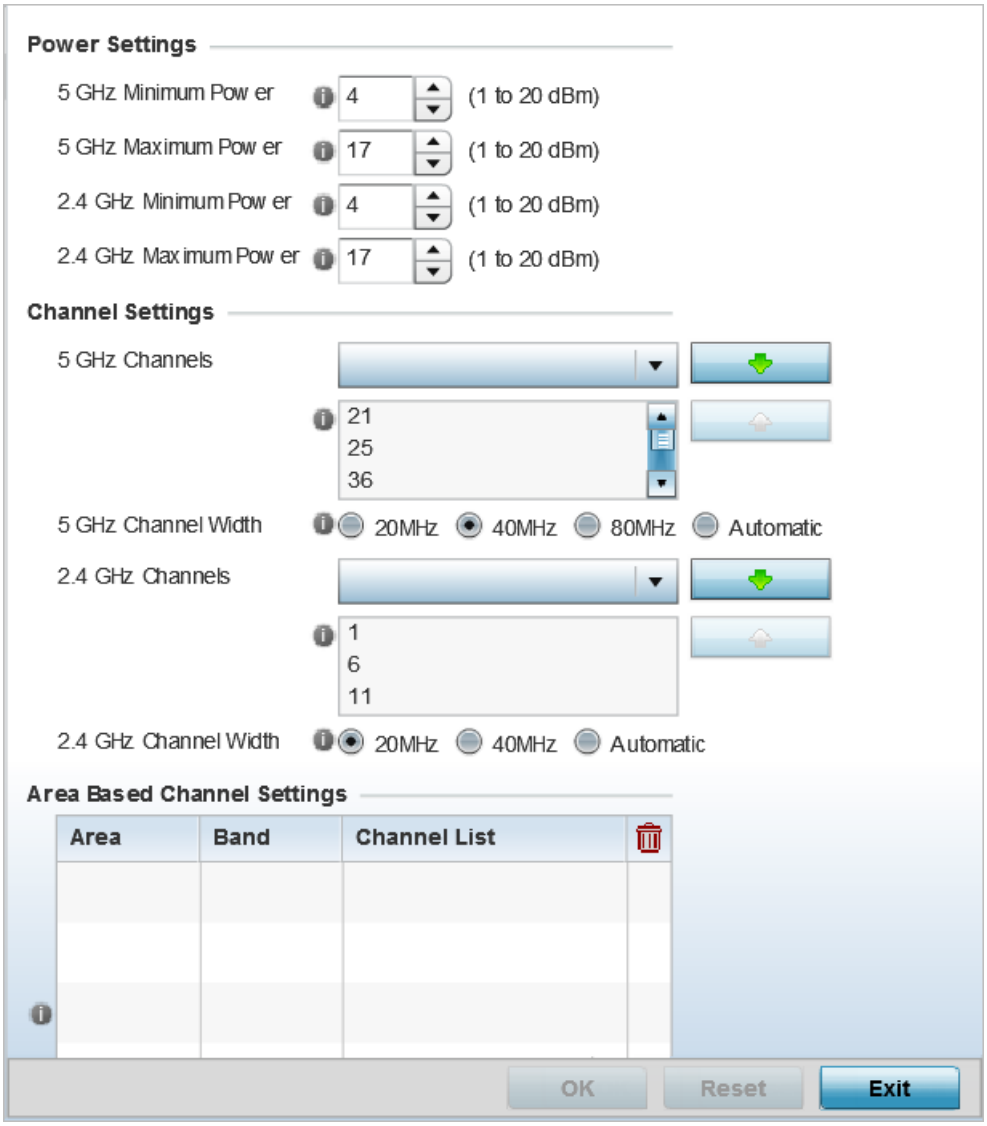



**Figure 312: SMART RF - Channel and Power Screen**

2 Refer to the **Power Settings** field to define Smart RF recovery settings for the selected 5.0 GHz (802.11a) or 2.4 GHz (802.11bg) radio.

| | |
|---|---|
| 5 GHz Minimum Power | Use the spinner control to select a 1 - 20 dBm minimum power level for Smart RF to assign to a radio in the 5.0 GHz band. The default setting is 4 dBm. |
| 5 GHz Maximum Power | Use the spinner control to select a 1 - 20 dBm maximum power level Smart RF can assign a radio in the 5.0 GHz band. The default setting is 17 dBm. |
| 2.4 GHz Minimum Power | Use the spinner control to select a 1 - 20 dBm minimum power level Smart RF can assign a radio in the 2.4 GHz band. The default setting is 4 dBm. |
| 2.4 GHz Maximum Power | Use the spinner control to select a 1 - 20 dBm maximum power level Smart RF can assign a radio in the 2.4 GHz band. The default setting is 17 dBm. |

3 Set the following **Channel Settings** for the 5.0 GHz and 2.4 GHz radios.

| | |
|---|---|
| 5 GHz Channels | Use the Select drop-down menu to define the 5 GHz channels used for Smart RF assignments. |
| 5 GHz Channel Width | 20 and 40 MHz channel widths are supported by the 802.11a radio. 20/ 40 MHz operation (the default setting for the 5 GHz radio) allows the access point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select **`Automatic`** to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. 40MHz is the default setting. |
| 2.4 GHz Channels | Set the 2.4 GHz channels used in Smart RF scans. |
| 2.4 GHz Channel Width | 20 and 40 MHz channel widths are supported by the 802.11a radio. 20 MHz is the default setting for 2.4 GHz radios. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the access point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select **`Automatic`** to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. 20MHz is the default setting. |

4 Select **+ Add Row** and set the following **Area Based Channel Settings** for the Smart RF policy:

| | |
|---|---|
| Area | Use the text area to provide a name for the area being configured. |
| Band | Select the radio band, either 2.4 GHz or 5 GHz, for the Smart RF policy assigned to the specified area. |
| Channel List | Select the channels associated with the Smart RF policy for the specified area and band. |

5 Click **OK** to update the Smart RF and Power settings for this policy.

Click **Reset** to revert to the last saved configuration.

The Smart RF policy can be invoked at any point in the configuration process by selecting **Activate SMART RF Policy** from the upper, left-hand portion of the access point user interface.

## Configuring Smart RF Scanning Configuration

To configure the Smart RF scanning configuration:

1 Select **Scanning Configuration**.

Ensure that **Activate SMART RF Policy** remains selected so that the screen's parameters can be updated. Additionally, the Smart RF configuration cannot be applied to the access point profile unless this setting remains selected.

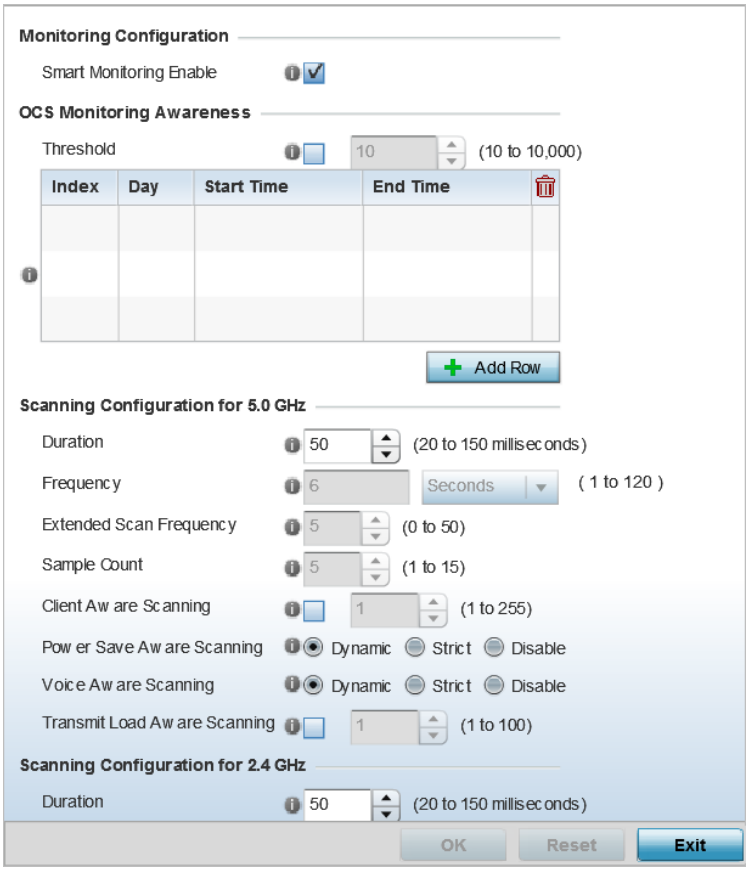



**Figure 313: SMART RF - Scanning Configuration Screen**

Note
The monitoring and scanning parameters in the Scanning Configuration screen are enabled only when **Custom** is selected as the **Sensitivity** setting from the Basic Configuration screen.

2 Enable or disable **Smart Monitoring Enable**.

The feature is enabled by default. When it is enabled, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.

3 Select **+ Add Row** and set **OCS Monitoring Awareness Settings** for the Smart RF policy:

| | |
|---|---|
| Threshold | Select this option and specify a threshold from 10 - 10,000. When the threshold is reached awareness settings are overridden with the values specified in the table. |
| Index | Select an Index value from 1 - 3 for awareness overrides. The overrides are executed based on index, with the lowest index being executed first. |
| Day | Use the drop-down menu to select a day of the week to apply the override. Selecting **All** will apply the policy every day. Selecting **weekends** will apply the policy on Saturdays and Sundays only. Selecting **weekdays** will apply the policy on Monday, Tuesday, Wednesday, Thursday and Friday. Selecting individual days of the week will apply the policy only on the selected days. |
| Start Time | Set the starting time of day when the overrides will be activated. Use the spinner controls to select the hour and minute, in 12h time format. Then use the radio button to choose **AM** or **PM**. |
| End Time | Set the ending time of day when the overrides will be disabled. Use the spinner controls to select the hour and minute, in 12h time format. Then use the radio button to choose **AM** or **PM**. |

4 Set the following **Scanning Configurations** for both the 2.4 and 5.0 GHz radio bands:

| | |
|---|---|
| Duration | Set a channel scan duration (from 20 - 150 milliseconds) that access point radios use to monitor devices within the network and, if necessary, perform self healing and neighbor recovery to compensate for coverage area losses within an RF Domain. The default setting is 50 milliseconds for both 2.4 GHz and 5.0 GHz bands. |
| Frequency | Set the scan frequency using the drop-down menu. Set a scan frequency in either seconds (1 - 120) or minutes (0 - 2). The default setting is 6 seconds for both the 5 and 2.4 GHz bands. |
| Extended Scan Frequency | Use the spinner control to set an extended scan frequency between 0 - 50. This is the frequency on which radios scan channels on other than their peer radios. The default setting is 5 for both the 5 and 2.4 GHz bands. |
| Sample Count | Use the spinner control to set a sample scan count value between 1 - 15. This is the number of RF readings a radio gathers before it sends the data to the Smart RF master. The default setting is 5 for both the 5 and 2.4 GHz bands |
| Client Aware Scanning | Set a client awareness count (1 - 255) during off channel scans for either the 2.4 or 5.0 GHz radio. The default setting is 1 for both radio bands. |
| Power Save Aware Scanning | Select either the **Dynamic**, **Strict**, or **Disable** radio button to define how power save scanning is set for Smart RF. **Strict** disables smart monitoring as long as a power save capable client is associated to a radio. **Dynamic** disables smart monitoring as long as there is data buffered for a power save client at the radio. The default setting is **Dynamic** for both the 5 and 2.4 GHz bands. |
| Voice Aware Scanning | Select either the **Dynamic**, **Strict**, or **Disable** radio button to define how voice aware recognition is set for Smart RF. **Strict** disables smart monitoring as long as a power save capable client is associated to a radio. **Dynamic** disables smart monitoring as long as there is data buffered for a voice client at the radio. The default setting is **Dynamic** for both the 5 and 2.4 GHz bands. |
| Transmit Load Aware Scanning | Select this option to set a transmit load percentage from 1 - 100 serving as a threshold before scanning is avoided for an access point's 2.4 GHz radio. |

5 Click **OK** to update the Smart RF Scanning Configuration settings for this policy.

Click **Reset** to revert to the last saved configuration.

## Configuring Smart RF Neighbor Recovery Settings

To configure Smart RF recovery settings:

1 Select **Recovery**.

The Neighbor Recovery tab displays by default. Use the Neighbor, Interference, and Coverage Hole recovery tabs to define how 2.4 and 5.0 GHz radios compensate for failed neighbor radios, interference, coverage holes, and loss of root path requiring intervention by neighbor radios.

2 Use the **Power Hold Time** field to define the minimum time between two radio power changes during neighbor recovery.

Set the time in either seconds (0 - 3,600), minutes (0 - 60) or hours (0 - 1). The default setting is 0 seconds.

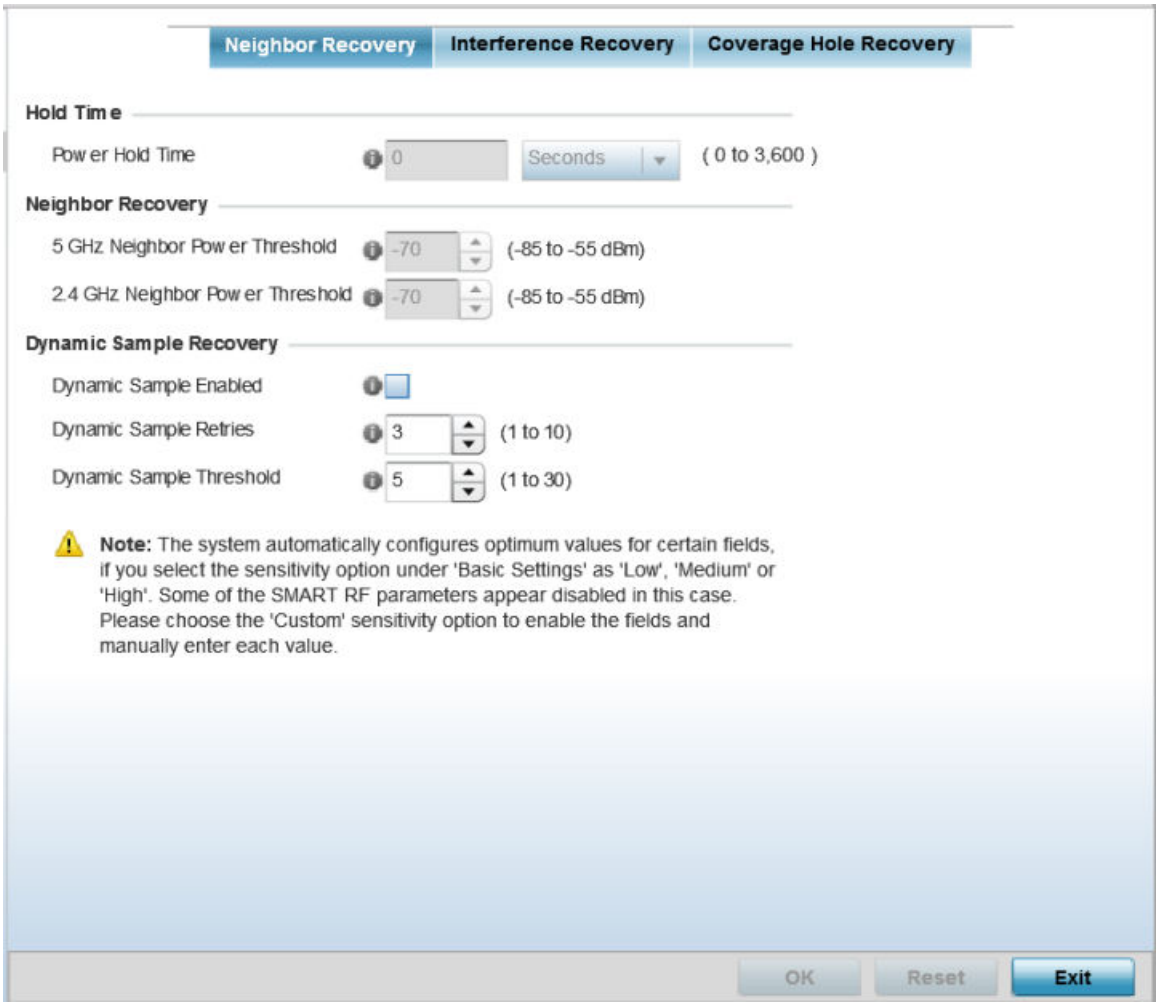



**Figure 314: SMART RF - Advanced Configuration Screen - Neighbor Recovery Tab**

3 Set the following **Neighbor Recovery** parameters:

Note

The recovery parameters within the Neighbor Recovery, Interference and Coverage Hole Recovery tabs are enabled only when **Custom** is selected as the **Sensitivity** setting from the Smart RF Basic Configuration screen.

| | |
|---|---|
| 5 GHz Neighbor Power Threshold | Set the maximum power increase threshold (from -85 to -55 dBm) the access point's 5.0 GHz radio uses if it is required to increase its output power to compensate for a failed radio within the access point's radio coverage area. The default value is -70 dBm. |
| 2.4 GHz Neighbor Power Threshold | Set the maximum power increase threshold (from -85 to -55 dBm) the access point's 2.4 GHz radio uses if it is required to increase its output power to compensate for a failed radio within the access point's radio coverage area. The default value is -70 dBm. |

4 Set the following **Dynamic Sample Recovery** parameters:

| | |
|---|---|
| Dynamic Sample Enabled | Select this option to enable dynamic sampling. Dynamic sampling enables an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values. This option is disabled by default. |
| Dynamic Sample Retries | Set the number of retries (from 1 - 10) attempted before a power level adjustment is implemented to compensate for a potential coverage hole. The default setting is 3. |
| Dynamic Sample Threshold | Set the number of sample reports (1 - 30) used before dynamic sampling is invoked for a potential power change adjustment. The default setting is 5. |

5 Click **OK** to update the Smart RF Neighbor Recovery settings for this policy.

Click **Reset** to revert to the last saved configuration.

### *Configuring Smart RF Interference Recovery Settings*

To configure Smart RF Interference Recovery Settings:

1 Select **Interference Recovery**.

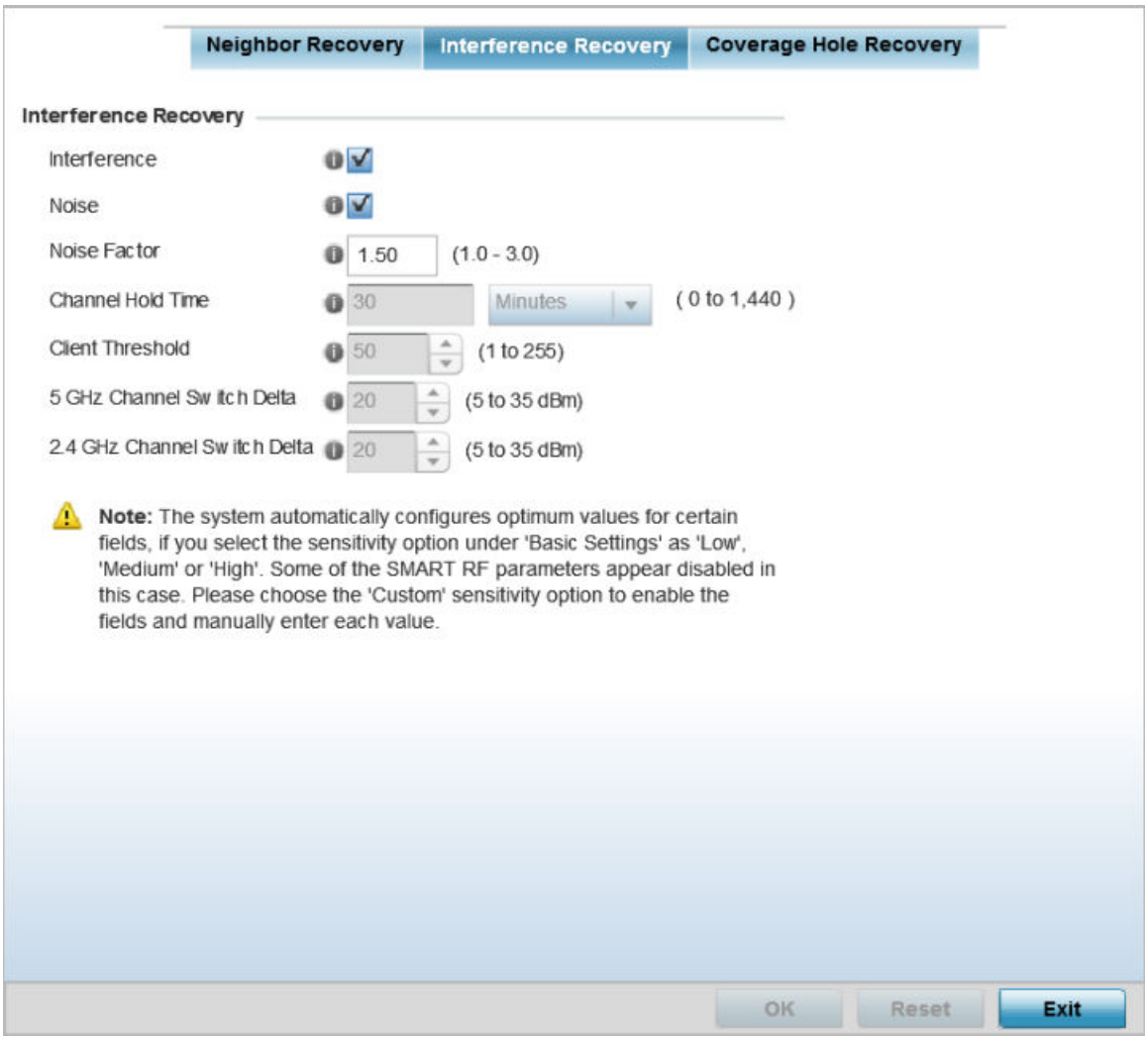



**Figure 315: SMART RF - Advanced Configuration Screen - Interference Recovery Tab**

2 Set the following **Interference Recovery** parameters:

| | |
|---|---|
| Interference | Select this option to allow the Smart RF policy to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a cleaner channel. This feature is enabled by default. |
| Noise | Select this option to allow the Smart RF policy to scan for excess noise from WiFi devices. When detected, Smart RF supported access points can change their channel and move to a cleaner channel. This feature is enabled by default. |
| Noise Factor | Set the noise factor (level of network interference detected) taken into consideration by Smart RF during interference recovery calculations. Set a value from 1.0 - 3.0. |
| Channel Hold Time | Define the minimum time between channel changes during neighbor recovery. Set the time in either seconds (0 - 86,400), minutes (0 - 1,440), hours (0 - 24), or days (0 - 1). The default setting is 30 minutes. |

| | |
|---|---|
| Client Threshold | Set a client threshold for the Smart RF policy between 1 - 255. If the set threshold number of clients are connected to a radio, the radio does not change its channel, even though required, based on the interference recovery determination made by the smart master. The default setting is 50. |
| 5 GHz Channel Switch Delta | Set a channel switch delta (interference delta), from 5 - 35 dBm, for the 5.0 GHz radio. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm. |
| 2.4 GHz Channel Switch Delta | Set a channel switch delta (interference delta), from 5 - 35 dBm, for the 2.4 GHz radio. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm. |

3 Click **OK** to update the Smart RF Interference Recovery settings for this policy.

Click **Reset** to revert to the last saved configuration.

*Configuring Smart RF Coverage Hole Recovery Settings*

1 Select **Coverage Hole Recovery**.

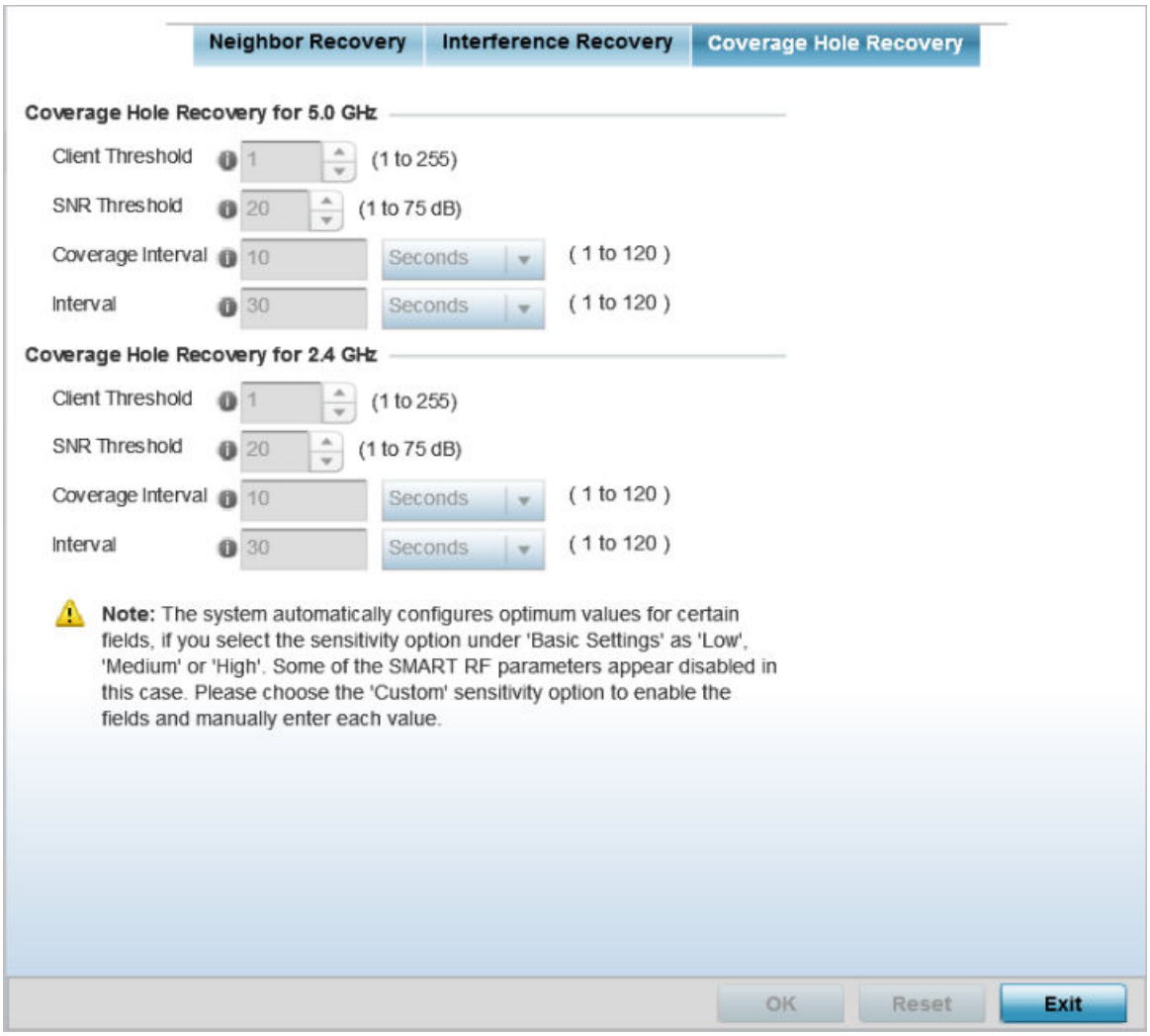



**Figure 316: SMART RF - Advanced Configuration Screen - Coverage Hold Recovery Tab**

2 Set the following **Coverage Hole Recovery for 2.4 GHz and 5.0 GHz** parameters:

| | |
|---|---|
| Client Threshold | Use the spinner to set a client threshold for the Smart RF policy between 1 - 255. This is the minimum number of clients a radio should have associated in order for coverage hole recovery to trigger. AP 6522, AP6522M, AP 6532, AP 6562, AP 7161, and AP 8132 model access points can support up to 256 clients per access point or radio.The default setting is 1. |
| SNR Threshold | Set a *signal-to-noise* (SNR) threshold , between 1 - 75 dB. This is the signal-to-noise threshold for an associated client as seen by its associated access point radio. When exceeded, the radio increases its transmit power in order to increase coverage for the associated client. The default value is 20 dB. |

| | |
|---|---|
| Coverage Interval | Define the length of time after which coverage hole recovery should be initiated when a coverage hole is detected. The default is 10 seconds for both the 2.4 and 5.0 GHz radios. |
| Interval | Define the length of time coverage hole recovery should be conducted before a coverage hole is detected. The default is 30 seconds for both the 2.4 and 5.0 GHz radios. |

3 Click **OK** to update the Smart RF Coverage Hole Recovery settings for this policy.

Click **Reset** to revert to the last saved configuration.

## Configuring Smart RF Select Shutdown Settings

To enable Smart RF select and shutdown 2.4 GHz APs causing interefrence:

1 Select **Select Shutdown**,

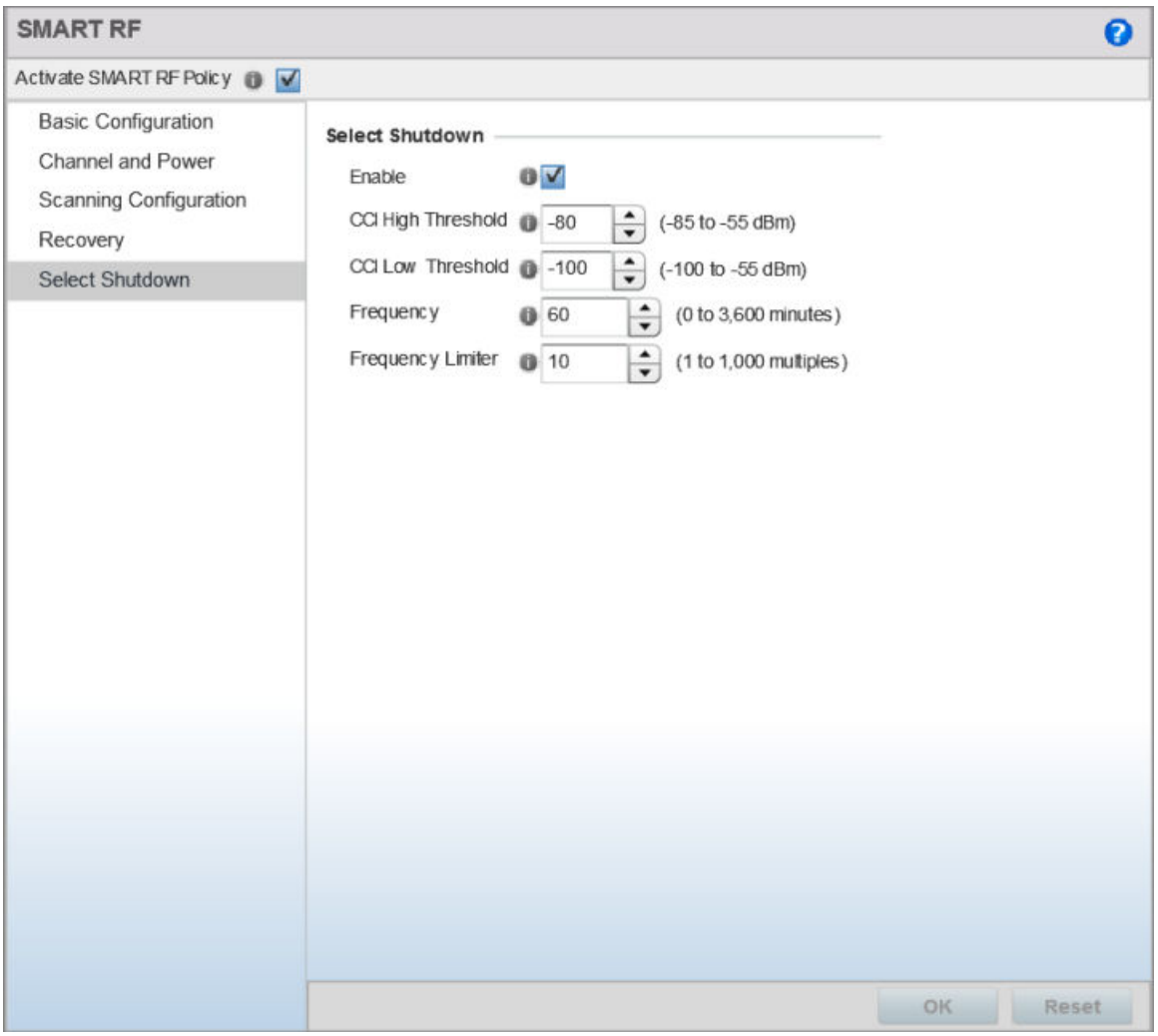



**Figure 317: Smart RF Configuration - Select Shutdown screen**

2 Configure the following parameters that will maintain CCI *(co-channel interference)* levels within specified limits.

| | |
|---|---|
| Enable | Select to enable auto-shutdown of radios causing interference within the Smart RF monitored network.<br>Auto-shutdown of select 2.4 GHz radios, in dual-band networks, maintains CCI levels within specified limits. When enabled, Smart-RF monitors CCI levels to ensure that the deployment average CCI remains within specified minimum and maximum limits. If the deployment average CCI is found to exceed the maximum threshold, 2.4 GHz radios, causing neighbor interference, are shut down one-by-one until the deployment average CCI falls below the specified maximum threshold. The reverse process occurs when the deployment average CCI falls below the minimum threshold. In this scenario, previously disabled radios are enabled until the deployment average CCI reaches acceptable levels.<br><br>Note: This feature is enabled by default. |
| CCI High Threshold | Specify the maximum CCI threshold from -85 to -55 dBm. The default value is -80 dBm.<br><br>Note: If not specified, the system uses the default value as the upper limit for the deployment average CCI range. |
| CCI Low Threshold | Specify the minimum CCI threshold from -85 to -55 dBm. The default value is -100 dBm.<br><br>Note: If not specified, the system uses the default value as the lower limit for the deployment average CCI range. |
| Frequency | Configure the interval, in minutes, at which 2.4 GHz radios are selected for shut down. when the deployment average CCI exceeds the specified maximum threshold, Smart RF shuts down 2.4 GHz radios until the CCI reaches acceptable levels. Use this option, to configure the interval between successive radio shut down.<br>Specify the frequency from 0 - 3600 minutes. The default is 60 minutes. |
| Frequency Limiter | Configure the minimum multiple of Interference Recovery frequency that the select-shutdown frequency can be set to.<br>Specify a value from 1 - 1000. The default value is 15. |

3 Click **OK** to update the Smart RF Select Shutdown settings for this policy.

Click **Reset** to revert to the last saved configuration.

## Smart RF Configuration and Deployment Considerations

Before defining a Smart RF policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Smart RF cannot detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections.
- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when access points are

deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

Keep in mind, if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.
- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks a channel specified in the Smart RF policy.
- If no Smart RF policy is mapped, the radio selects a random channel.

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access points detects radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using a `no dfs-rehome` command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

## MeshConnex Policies

*MeshConnex* is a mesh networking technology that is comparable to the 802.11s mesh networking specification. MeshConnex meshing uses a hybrid proactive/on-demand path selection protocol, similar to *Ad hoc On Demand Distance Vector* (AODV) routing protocols. This allows it to form efficient paths using multiple attachment points to a distribution WAN, or form purely ad hoc peer-to-peer mesh networks in the absence of a WAN. Each device in the MeshConnex mesh proactively manages its own path to the distribution WAN, but can also form peer-to-peer paths on demand to improve forwarding efficiency. MeshConnex is not compatible with MiNT-based meshing, though the two technologies can be enabled simultaneously in certain circumstances.

MeshConnex is designed for large-scale, high-mobility outdoor mesh deployments. MeshConnex continually gathers data from beacons and transmission attempts to estimate the efficiency and throughput of each MP-to-MP link. MeshConnex uses this data to dynamically form and continually maintain paths for forwarding network frames.

In MeshConnex systems, a *mesh point* (MP) is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 MPs can be created and 2 can be created per radio. MPs can be configured to use one or both radios in the device. If the MP is configured to use both radios, the path selection protocols will continually select the best radio to reach each destination. Each MP participates in a single Mesh Network, defined by the MeshID. The MeshID is typically a descriptive network name, similar to the SSID of a WLAN. All MPs configured to use the same MeshID attempt to form a mesh and interoperate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

Note
WiNG 7.1 release does not support MeshConnex on AP505i and AP510i model access points. This feature will be supported in future releases.

## Configuring a MeshConnex Policy

To define a MeshConnex policy:

1 Select **Configuration** > **Wireless** > **MeshConnex Policy** tto display existing MeshConnex policies.

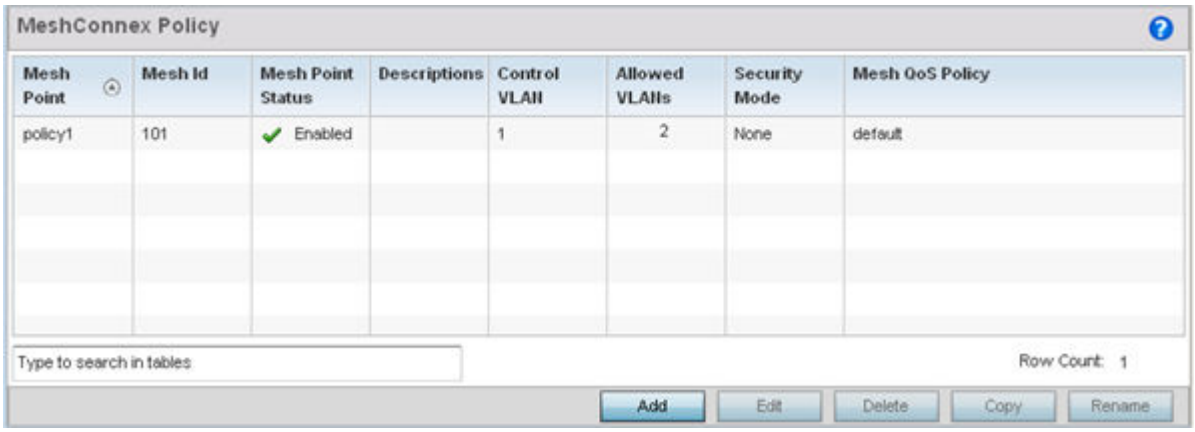



**Figure 318: MeshConnex Policy Screen**

2 Refer to the following configuration data for existing MeshConnex policies:

| | |
|---|---|
| Mesh Point Name | The names of all configured mesh points. |
| Mesh ID | The IDs (mesh identifiers) assigned to mesh points. |
| Mesh Point Status | Tthe status of each configured mesh point, either **Enabled** or **Disabled**. |
| Description | Descriptive text provided by the administrator for each configured mesh point. |
| Control VLAN | The VLAN (virtual interface ID) for the control VLAN on each of the configured mesh points. |
| Allowed VLANs | The list of VLANs allowed on each configured mesh point. |
| Security Mode | The security assigned to each configured mesh pointt – either **None** for no security or **PSK** for pre-shared key authentication. |
| Mesh QoS Policy | The mesh Quality of Service (QoS) policy associated with each configured mesh point. |

3 Click **Add** to create a new MeshConnex policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy.

Optionally, **Copy** or **Rename** MeshConnex policies as needed.

The Configuration screen displays by default for new or modified MeshConnex policies.

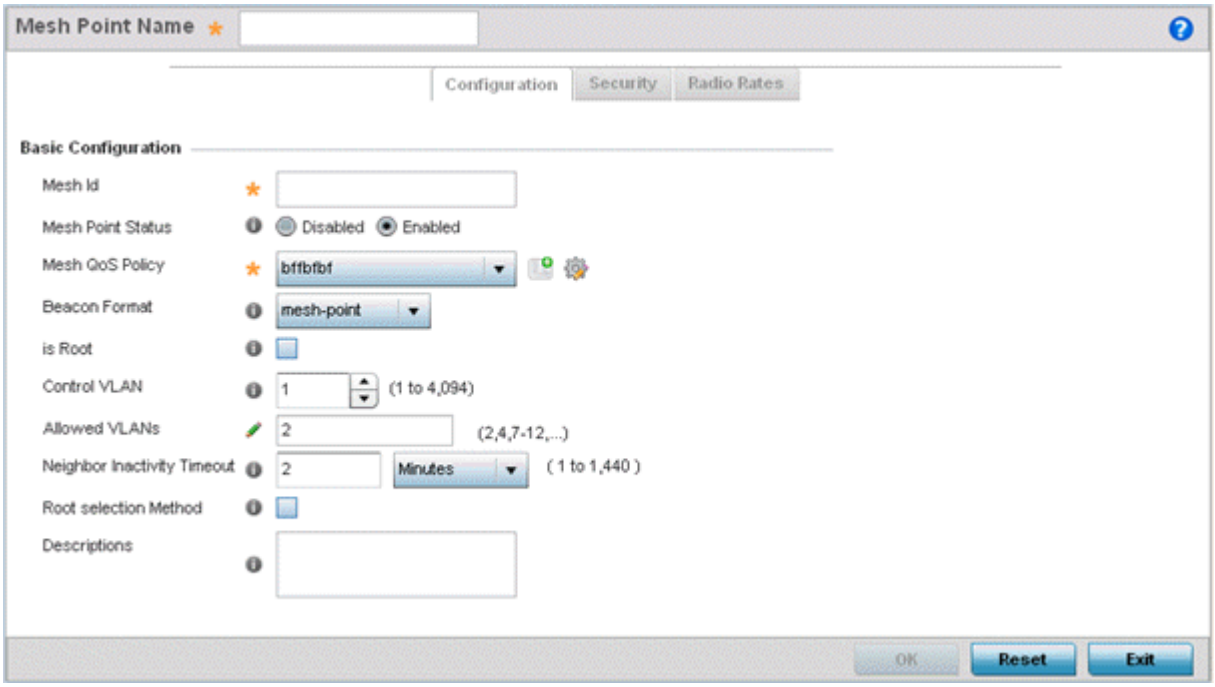



**Figure 319: MeshConnex Configuration Screen**

4 Refer to the **Basic Configuration** field to define a MeshConnex configuration:

| | |
|---|---|
| Mesh Point Name | Specify a name for the new mesh point. The name should be descriptive to easily differentiate it from other mesh points. This field is mandatory. |
| Mesh ID | Specify a 32-character maximum mesh identifier for this mesh point. This field is optional. |
| Mesh Point Status | To enable this mesh point, click **Enabled**. To disable the mesh point, click **Disabled**. The default value is **Enabled**. |
| Mesh QoS Policy | Specify the mesh Quality of Service (QoS) policy to use on this mesh point. This value is mandatory. If no suitable mesh QoS policies exist, click the **Create** icon to create a new mesh QoS policy. |
| Beacon Format | Specify the format in which beacons from the mesh point are sent. To use access point style beacons, select **access-point** from the drop-down menu. To use mesh point style beacons, select **mesh point**. The default value is **mesh point**. |
| Is Root | Select this option to define the mesh point as a root in the mesh topology. |
| Control VLAN | Specify a VLAN to carry meshpoint control traffic. The valid range for control VLAN is between 1 and 4094. The default value is VLAN 1. |

| | |
|---|---|
| Allowed VLANs | Specify the VLANs that are allowed to pass traffic on the mesh point. Separate VLANs with commas. To specify a range of allowed VLANs, separate the starting VLAN and the ending VLAN with a hyphen. Aliases can be used to configure Allowed VLANs. |
| Neighbor Inactivity Timeout | Specify the amount of time allowed between frames received from a neighbor before their client privileges are revoked. Specify the timeout value in seconds, minutes, hours or days, up to a maximum of 1 day. The default value is 2 minutes. |
| Description | Enter a 64-character maximum description for the mesh point configuration. |

5 Click **OK** to update the MeshConnex configuration settings for this policy.

Click **Reset** to revert to the last saved configuration.

6 Select **Security**.

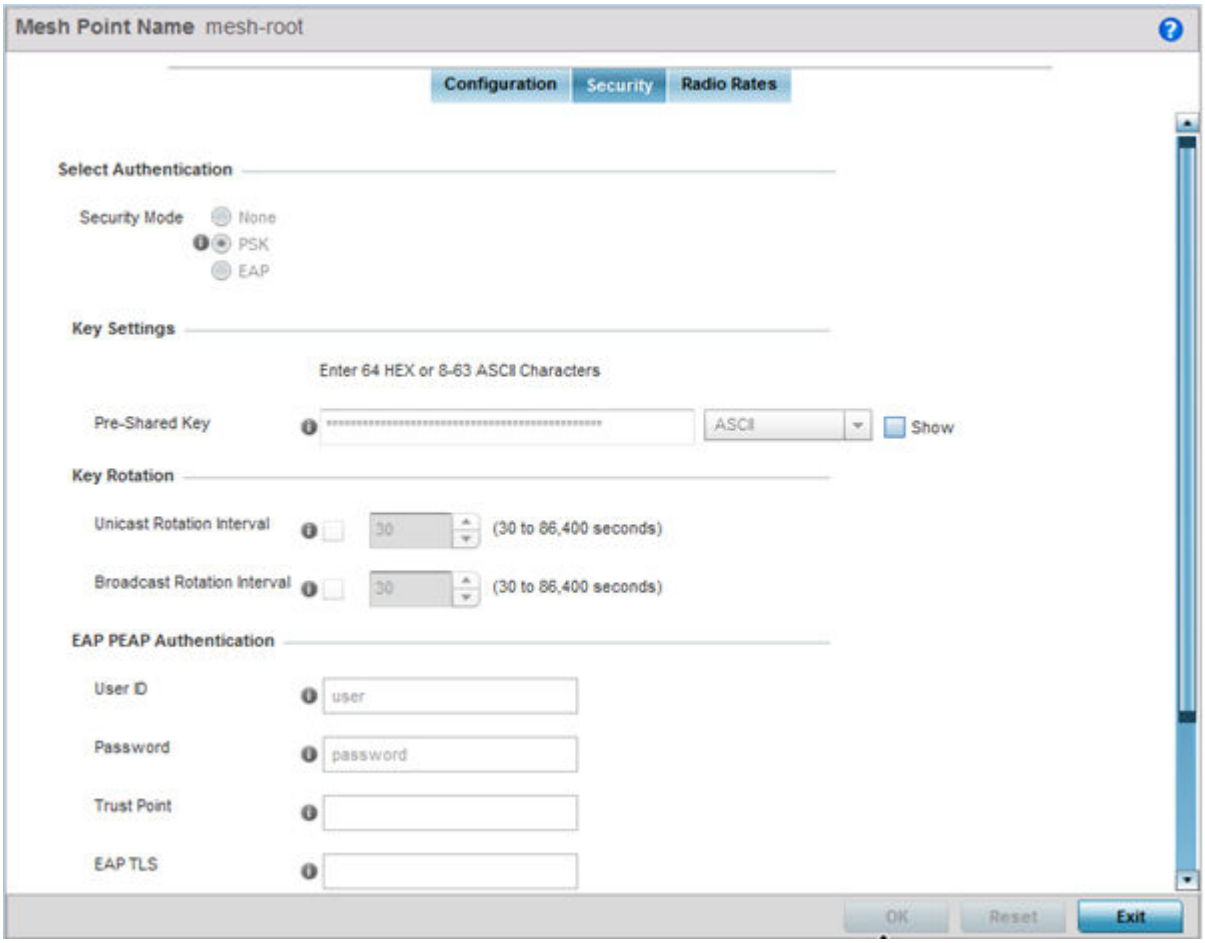



**Figure 320: MeshConnex Security Screen**

7 Refer to the **Select Authentication** field to define an authentication method for the mesh policy.

| | |
|---|---|
| Security Mode | Select a security authentication mode for the mesh point. Select **None** to have no authentication for the mesh point. Select **PSK** to set a pre-shared key as the authentication for the mesh-point. If **PSK** is selected, enter a pre-shared key in the **Key Settings** field. The default setting is **None**. |

8 Set the following **Key Settings** for the mesh point.

| | |
|---|---|
| Pre-Shared Key | When the security mode is set as **PSK**, enter a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point. |

9 Set the following **Key Rotation** settings for the mesh point.

| | |
|---|---|
| Unicast Rotation Interval | Define an interval for unicast key transmission (30 -86,400 seconds). This option is disabled by default. |
| Broadcast Rotation Interval | When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in seconds (30- 86,400). Key rotation enhances the broadcast traffic security on the WLAN. This option is disabled by default. |

10 If you are using EAP to secure the mesh point, set the following **EAP PEAP Authentication** settings.

| | |
|---|---|
| User ID | Create a 32-character maximum user name for a *peap-mschapv2* authentication credential exchange. |
| Password | Define a 32-character maximum password for the EAP PEAP user ID. |
| Trust Point | Provide the 64 character maximum name of the trustpoint used for installing the CA certificate and validating the server certificate. |
| EAP TLS | Provide the 64 character maximum name of the trustpoint used for installing the client certificate, client private key and CA certificate. |
| Type | Configure the EAP authentication method used by supplicants. The options are **PEAP-MSCHAPv2** and **TLS**. |
| EAP Identity | Configure the EAP identity used during phase1 authentication. The value configured here need not the user's actual identity. |
| AAA Policy | Specify the AAA policy used with this EAP PEAP Authentication. Use the **Create** or **Edit** buttons to create a new AAA policy or edit and existing AAA policy. |

11 Click **OK** to save the changes made to the configuration.

Click **Reset** to revert to the last saved configuration.

12 Select **Radio Rates**.

13 Set the following **Radio Rates** for both the 2.4 and 5 GHz radio bands:

| | |
|---|---|
| 2.4 GHz Mesh Point | Click **Select** to configure radio rates for the 2.4 GHz band. Define both minimum **`Basic`** and optimal **`Supported`** rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band.<br>If you are supporting 802.11n, select a Supported MCS index. Set an MCS (*modulation and coding scheme*) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates).<br>The selected rates apply to associated client traffic within this mesh point only. |
| 5.0 GHz Mesh Point | Click **Select** to configure radio rates for the 5.0 GHz band. Define both minimum **`Basic`** and optimal **`Supported`** rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 5.0 GHz radio band.<br>If you are supporting 802.11n, select a Supported MCS index. Set an MCS (*modulation and coding scheme*) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates).<br>The selected rates apply to associated client traffic within this mesh point only. |

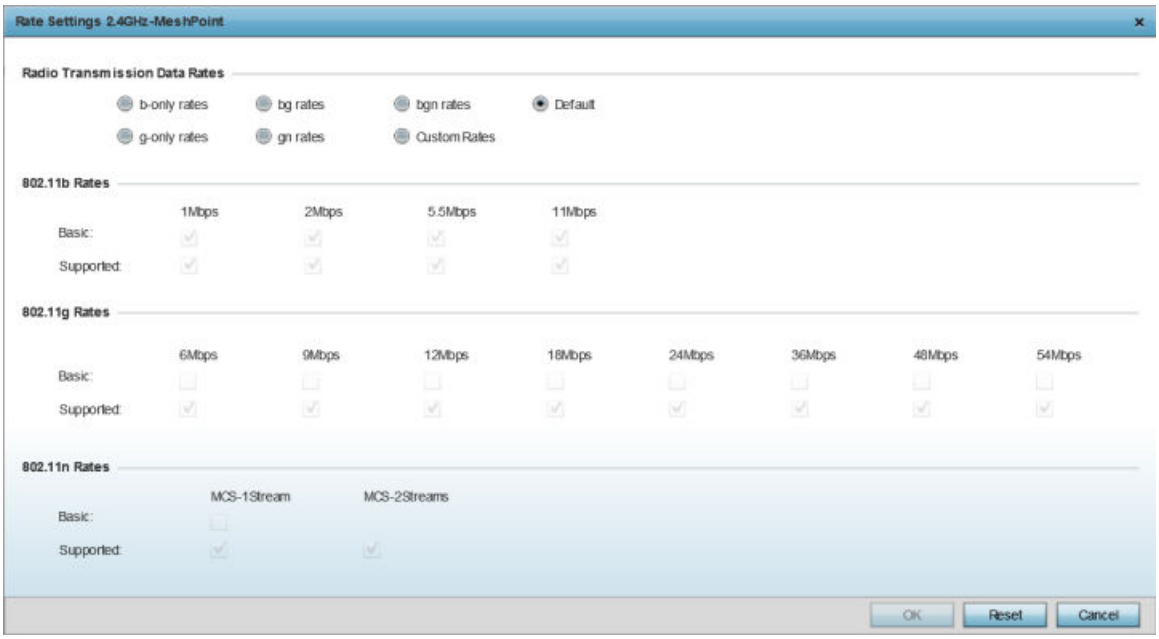



**Figure 321: Advanced Rate Settings 2.4 GHz Screen**

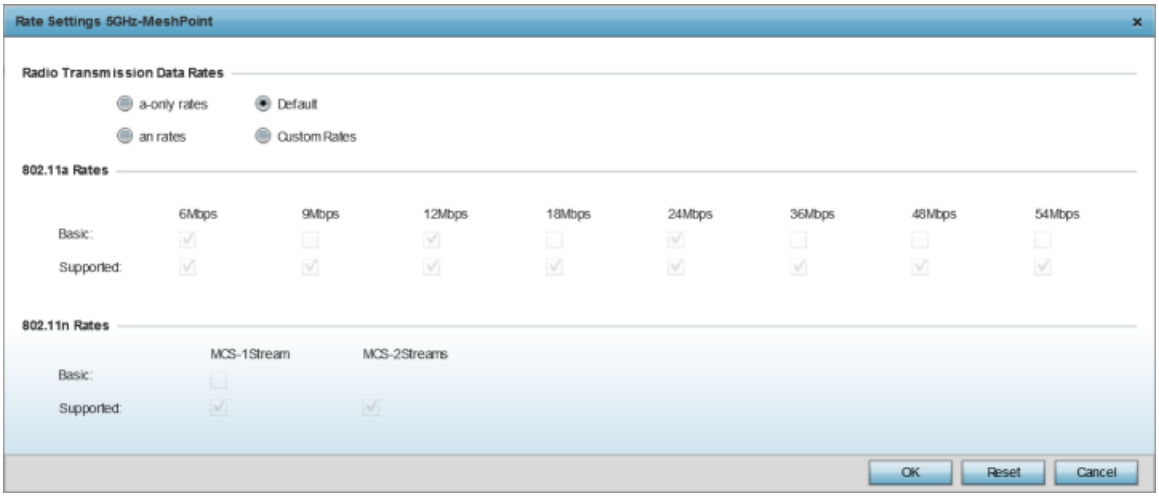



**Figure 322: Advanced Rate Settings 5.0 GHz Screen**

14 Define both minimum **Basic** and optimal **Supported** rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band and 802.11a and 802.11n rates supported by the 5.0 GHz radio band.

These are the rates wireless client traffic is supported within this mesh point.

If you are supporting 802.11n, select a Supported MCS index. Set an MCS (*modulation and coding scheme*) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

15 Click **OK** to save the changes made to the configuration.

Click **Reset** to revert to the last saved configuration.

## Mesh QoS Policy

*Mesh Quality of Service* (QoS) provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

Mesh QoS ensures that each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or per the proportion configured. Packets directed to clients are classified into data types (video, voice, data, and so forth). Packets within each category are processed based on the weight (prioritization) set for each mesh point.

The Quality of Service screen displays a list of mesh QoS policies available to mesh points. Each mesh QoS policy can be selected to edit its properties. If none of the exiting Mesh QoS policies supports an

ideal QoS configuration for the intended data traffic of this mesh point, click **Add** to create a new policy. Select an existing mesh QoS policy and select **Edit** to change the properties of the mesh QoS policy.

Note
WiNG 7.1 release does not support MeshConnex on AP505i and AP510i model access points. This feature will be supported in future releases.

## Configuring a Mesh QoS Policy

To define a mesh QoS policy:

1 Select **Configuration → Wireless → Mesh QoS Policy** to display existing mesh QoS policies.

The Mesh Quality of Service (QoS) screen displays.

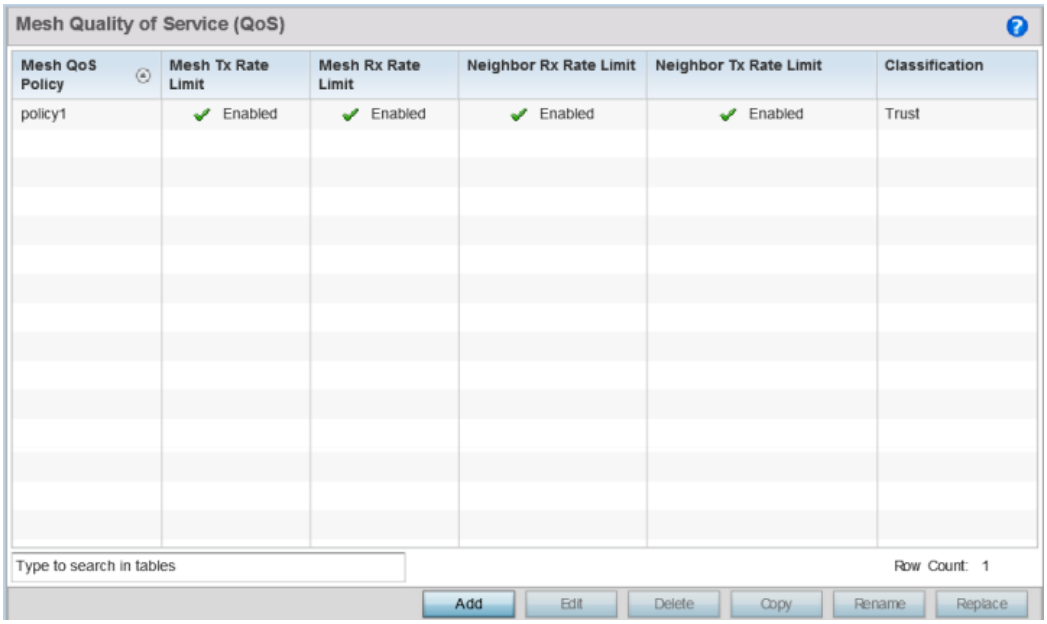



**Figure 323: Mesh QoS Policy Screen**

2 Refer to the following configuration data for existing mesh QoS policies:

| | |
|---|---|
| Mesh QoS Policy | The names of each configured mesh QoS policy. |
| Mesh Tx Rate Limit | Whether a **Mesh Tx Rate Limit** is enabled for each mesh QoS policy. This indicates rate limiting is enabled or disabled for all data received from any mesh point in the mesh. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled. |
| Mesh Rx Rate Limit | Whether a **Mesh Rx Rate Limit** is enabled for each mesh QoS policy. This indicates rate limiting is enabled or disabled for all data transmitted by the device to any mesh point in the mesh. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled. |
| Neighbor Rx Rate Limit | Whether a **Neighbor Rx Rate Limit** is enabled for each mesh QoS policy. This indicates rate limiting is enabled for data transmitted from connected wireless clients. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled. |

| | |
|---|---|
| Neighbor Tx Rate Limit | Whether a **Neighbor Tx Rate Limit** is enabled for each mesh QoS policy. This indicates rate limiting is enabled or disabled for data transmitted from the client to its associated access point radio and connected wireless controller. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled. |
| Classification | The forwarding QoS classification for each Mesh QoS policy. |

3 Click **Add** to define a new mesh QoS policy, select an existing policy and click **Edit** to modify it, or select an existing policy and click **Delete** to remove obsolete policy. Optionally, **Copy** or **Rename** mesh QoS policies as needed.
The Rate Limit screen displays by default for new or modified mesh QoS policies.

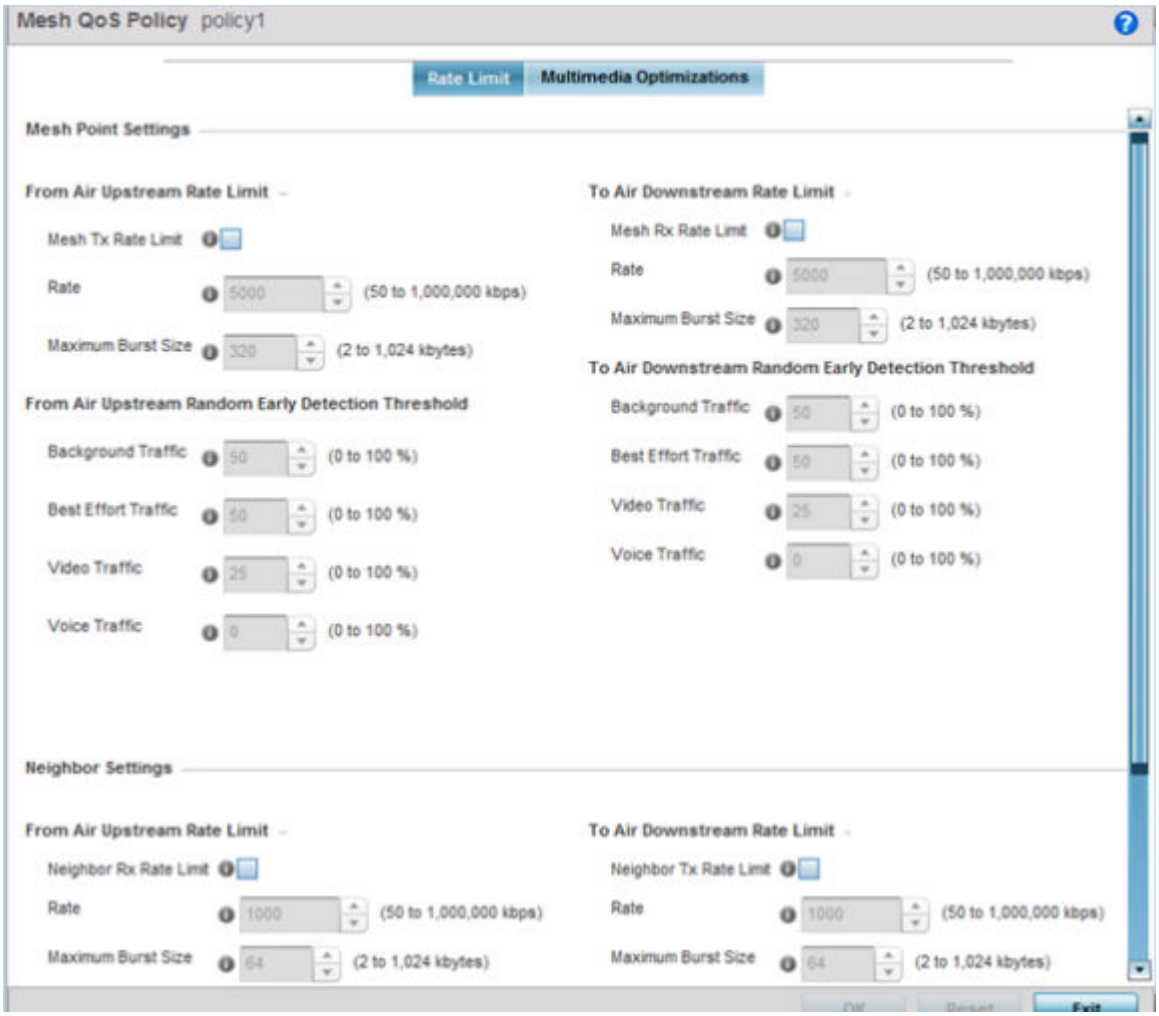



**Figure 324: Mesh QoS Policy Rate Limit Screen**

Excessive traffic can cause performance issues or bring down the network. Excessive traffic can be caused by network loops, faulty devices, or malicious software like a worm or virus that has infected one or more devices at the branch. By enabling rate limiting you can limit the maximum rate sent to or received from the wireless network (and mesh point) per neighbor. It prevents any single user from overwhelming the wireless network. It also provides differential service for service providers. You can set separate QoS rate limit configurations for data transmitted from the network and from a mesh point's neighbor back to their associated access point radios and managing controller or service platform.

Before you define rate limit thresholds for mesh point transmit and receive traffic, define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by enduser devices) is dropped, resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

4 Configure the following parameters for the **From Air Upstream Rate Limit**, or traffic from the controller to associated access point radios and their associated neighbor:

| | |
|---|---|
| Mesh Tx Rate Limit | Select this option to enable rate limiting for all data received from any mesh point in the mesh. This feature is disabled by default. |
| Rate | Define a receive rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received over the mesh point (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps. |
| Maximum Burst Size | Set a maximum burst size between 2 and 1024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the mesh point's client destinations. By trending the typical number of ARP, broadcast, multicast, and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320K bytes. |

5 Set the following **From Air Upstream Random Early Detection Threshold** settings, for each access category.

An early random drop occurs when a traffic stream falls below the set threshold.

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Video Traffic | Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the transmit direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. |

6 Configure the following parameters for the **To Air Upstream Rate Limit**, or traffic from neighbors to associated access point radios and the controller or service platform:

| | |
|---|---|
| Mesh Rx Rate Limit | Select this option to enable rate limiting for all data transmitted by the device to any mesh point in the mesh. This feature is disabled by default. |
| Rate | Define a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received over the mesh point (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps. |
| Maximum Burst Size | Set a maximum burst size between 2 and 1024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the mesh point's wireless client destinations. By trending the typical number of ARP, broadcast, multicast, and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320K bytes. |

7 Set the following **To Air Upstream Random Early Detection Threshold** settings, for each access category.

An early random drop occurs when the number of tokens for a traffic stream falls below the set threshold.

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. |
| Video Traffic | Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. |

8 Configure the following settings for **From Air Upstream Rate Limit** in the **Neighbor Settings** field:

| | |
|---|---|
| Neighbor Rx Rate Limit | Select this option to enable rate limiting for data transmitted from the client to its associated access point radio and connected controller or service platform. Enabling this option does not invoke client rate limiting for data traffic in the receive direction. This feature is disabled by default. |
| Rate | Define a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps. |
| Maximum Burst Size | Set a maximum burst size between 2 and 1024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 320K bytes. |

9 Configure the following settings for **From Air Upstream Random Early Detection Threshold** in the **Neighbor Settings** field:

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%. |
| Video Traffic | Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the transmit direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 0%, which implies that no early random drops will occur. |

10 Configure the following settings for **To Air Upstream Rate Limit**, or traffic from a controller or service platform to associated access point radios and the wireless client:

| | |
|---|---|
| Neighbor Tx Rate Limit | Select this option to enable rate limiting for data transmitted from connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the transmit direction. This feature is disabled by default. |
| Rate | Define a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 1,000 kbps. |
| Maximum Burst Size | Set a maximum burst size between 2 and 1024K bytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the wireless client. The default burst size is 320K bytes. |

11 Set the following **To Air Upstream Random Early Detection Threshold** settings for each access category:

| | |
|---|---|
| Background Traffic | Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%. |
| Best Effort Traffic | Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%. |
| Video Traffic | Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 25%. |
| Voice Traffic | Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 0%, which implies that no early random drops will occur. |

12 Click **OK** to update this mesh QoS rate limit settings.

Click **Reset** to revert to the last saved configuration.

13 Select **Multimedia Optimizations**.

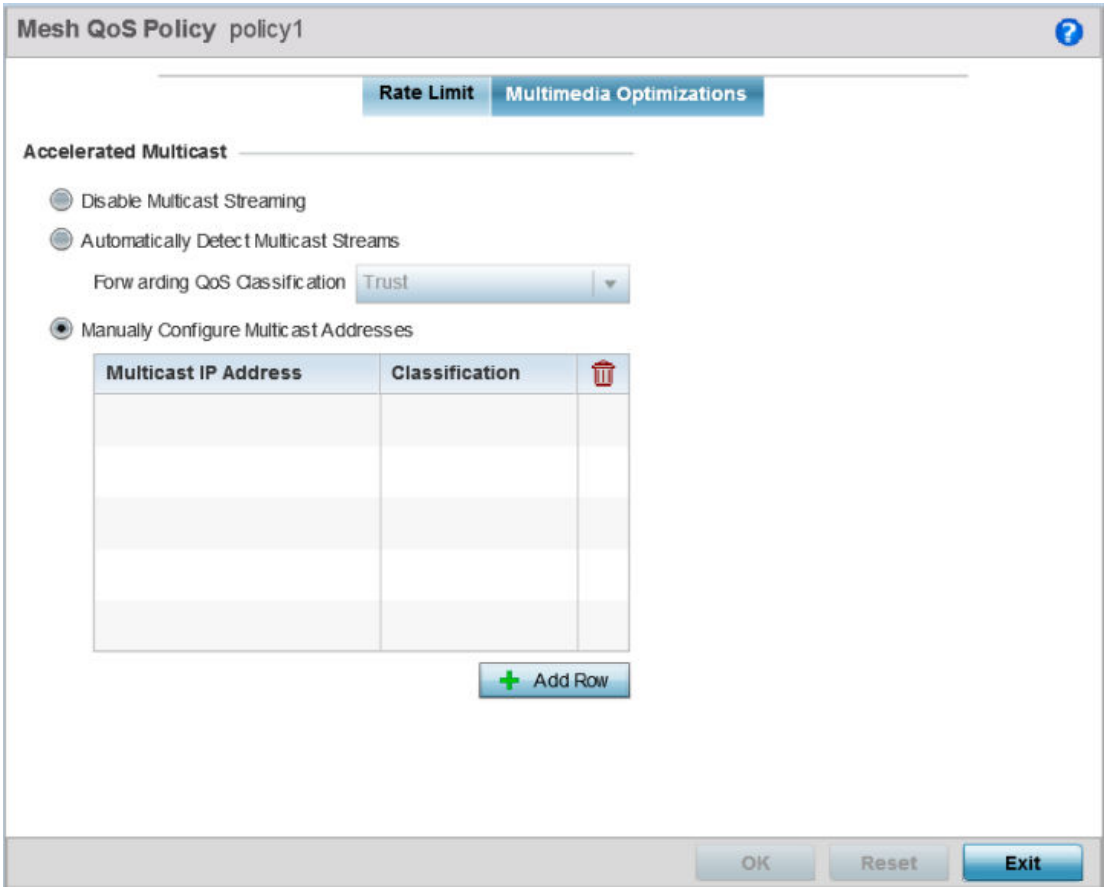



**Figure 325: Mesh QoS Policy Multimedia Optimizations Screen**

14 Set the following **Accelerated Multicast** settings:

| | |
|---|---|
| Disable Multicast Streaming | Select this option to disable all multicast streaming on the mesh point. |
| Automatically Detect Multicast Streams | Select this option to have bridged multicast packets converted to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, a number of classification mechanisms can be applied to the stream. The administrator can choose from the following classification types: **`Trust`**, **`Voice`**, **`Video`**, **`Best Effort`**, and **`Background`**. |
| Manually Configure Multicast Addresses | Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches. |

15 Click **OK** to update the Mesh Multimedia Optimizations settings.

Click **Reset** to revert to the last saved configuration.

## Passpoint Policy

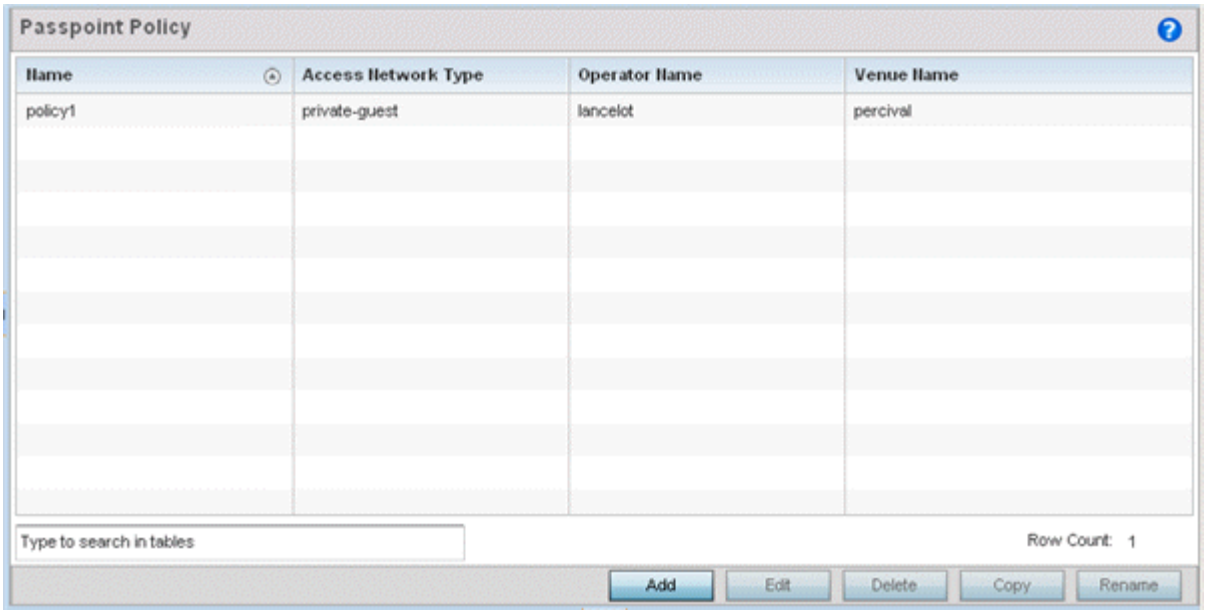
A *passpoint* policy provides a mechanism by which devices can select the correct network by querying for information from the available networks and then deciding which network to associate with. A passpoint policy is associated to a WLAN to enable the WLAN to provide hotspot services.

Passpoint makes connecting to Wi-Fi networks easier by authenticating the user with an account based on an existing relationship, such as the user's mobile carrier or broadband ISP.

A passpoint policy contains configuration that enables a client to query a network for information such as WAN metric, domain names and other relevant information. Only relevant information is presented to the client which enables it to decide with network to join.

To administrate and manage existing passpoint policies:

1 Select **Configuration → Wireless**.
2 Select Passpoint Policy from the Wireless node on the left-hand of the screen.




3 Refer to the following configuration data for existing passpoint policies:

| | |
|---|---|
| Name | Displays the administrator assigned name of each passpoint policy. |
| Access Network Type | Displays the network access permissions the administrator has set for the passpoint policy. |
| Operator Name | Displays the unique name assigned to the administrator or operator responsible for the configuration and operation of the hotspot. |
| Venue Name | Displays the administrator assigned name of the venue or physical location of the deployed hotspot. |

4 Select Add to define a new passpoint policy, or select an existing policy and select Edit to modify its configuration. Existing policies can be selected and deleted, copied, or renamed as needed.

## Configuring a Passpoint Policy

To create and manage passpoint policies:

1 Select **Configuration** > **Wireless** > **Passpoint Policy** to display existing passpoint policies.

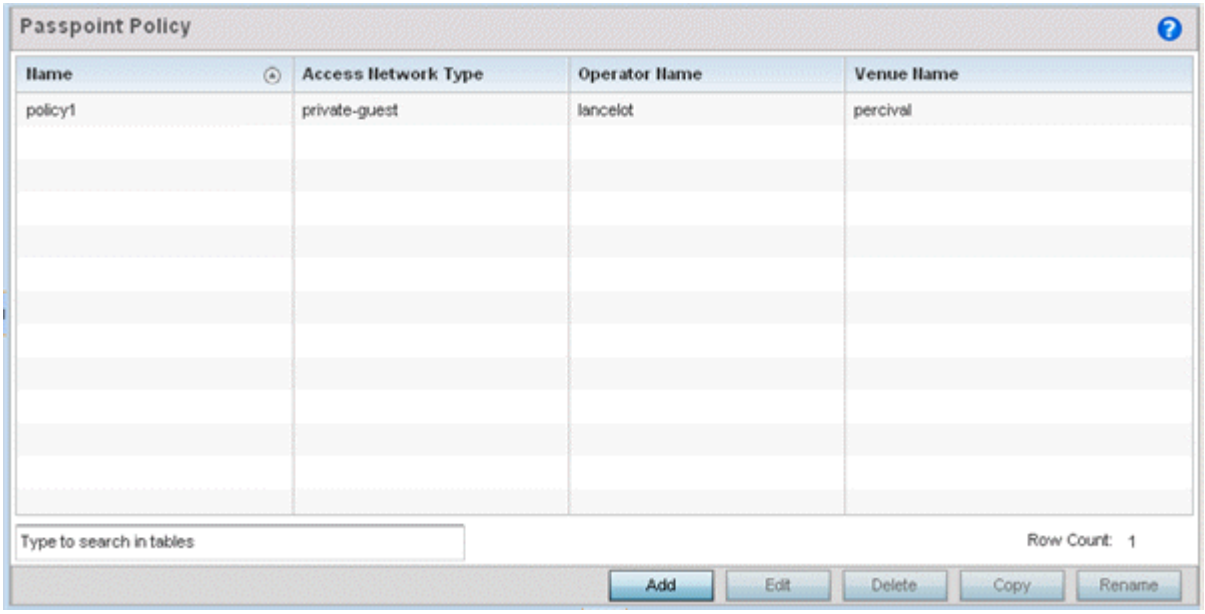



**Figure 326: Passpoint Policy Screen**

2 Refer to the following configuration data for existing passpoint policies:

| | |
|---|---|
| Name | The names of each configured passpoint policy. |
| Access Network Type | The type of hotspot which is advertised to all clients. |
| Operator Name | The name of the operator who manages the hotspot. |
| Venue Name | Information about the venue (or physical location) hosting the hotspot. |

3 Click **Add** to define a new passpoint policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy.

Optionally, **Copy** or **Rename** passpoint policies as needed.

The Configurations tab displays by default.

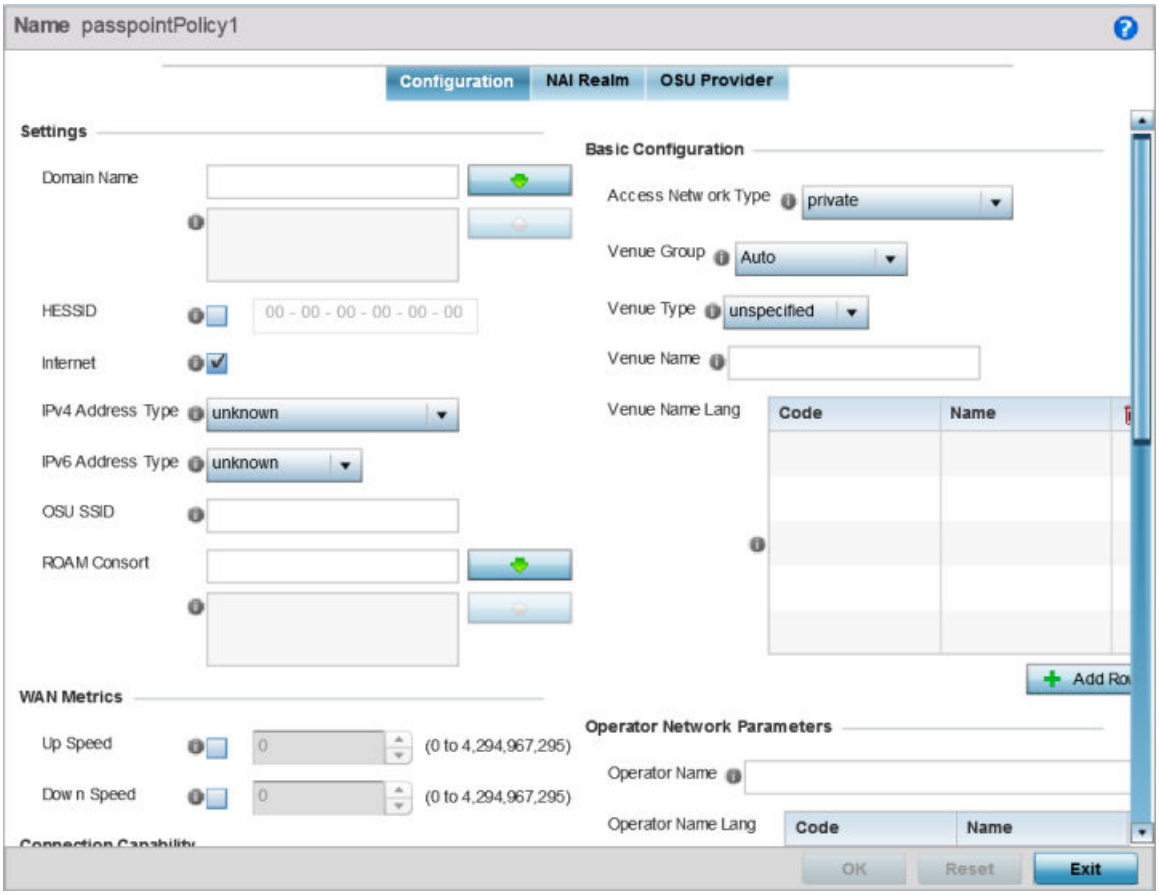



**Figure 327: Passpoint Policy - Configuration Screen**

4 Configure the following **Settings** to define an Internet connection medium for the passpoint policy

| | |
|---|---|
| Domain Name | Optionally, add a 255-character maximum domain name to the pool available to the passpoint policy. |
| HESSID | Select this option to apply a homogenous ESS ID. Leaving this option blank applies the BSSID instead. This option is disabled by default. |
| Internet | Select this option to enable Internet access to users of the passpoint hotspot. Internet access is enabled by default. |
| IPv4 Address Type | Select the IPv4 formatted address type for this passpoint policy. IPv4 is a connectionless protocol operating on a best effort delivery model. IPv4 does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP). Options include **`not available`**, **`public`**, **`port-restricted`**, **`port-restricted-double-nat`**, **`single-nat`**, **`double-nat`**, **`port-restricted-single-nat`**, and **`unknown`**. |

| | |
|---|---|
| IPv6 Address Type | Select the IPv6 formatted address type for this passpoint policy. IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. Options include **available**, **unavailable**, and **unknown**. |
| OSU SSID | Optionally define a 32 character maximum sign-on ID that must be correctly provided to access the passpoint policy's hotspot resources. |
| ROAM Consort | Provide a 0 - 255 character roaming consortium number. A roaming consort ID is sent as roaming consortium information in a hotspot query response. |

5 Set the following **WAN Metrics** for upstream and downstream bandwidth:

| | |
|---|---|
| Up Speed | Enable this option to estimate the maximum upstream bandwidth from 0 - 4,294,967,295 Kbps. |
| Down Speed | Enable this option to estimate the maximum downstream bandwidth from 0 - 4,294,967,295 Kbps. |

6 Set the following **Connection Capability** for the passpoint policy's FTP, HTTP, ICMP, IPSec VPN, PPTP VPN, SIP, SSH, and TLS VPN interfaces:

Use the drop-down menu to define these interfaces as **open**, **closed**, or **unknown** for this passpoint policy configuration. Disabling unused interfaces is recommended to close unnecessary security holes.

7 Select **+ Add Row** to set a **Connection Capability Variable** to make specific virtual ports **open** or **closed** for Wi-Fi connection attempts and to set rules for how the user can connect with routing preference using this passpoint policy.

8 Select **+ Add Row** and set a **Network Authentication Type** to select how Wi-Fi connection attempts are authenticated and validated using a dedicated redirection URL resource.

9 Refer to the **Basic Configuration** field to set the following:

| | | |
|---|---|---|
| Access Network Type | Select the network access method for this passpoint policy. Access network types include: | |
| | private | General access to a private network hotspot (default setting) |
| | private-guest | Access to a private network hotspot with guest services |
| | chargeable-public | Access to a public hotspot with billable services |
| | personal-device | Access to a hotspot for personal devices such as wireless routers |
| | emergency services | Dedicated network hotspot access for emergency services only |
| Venue Group | Passpoint is supported across a wide range of wireless network deployment scenarios and client devices. Select the group type best suited to the majority of hotspot requestors utilizing the passpoint policy's unique configuration. | |
| Venue Type | Select the venue type best suited to the actual location passpoint requestors are located. If an adequate option cannot be applied, a numeric venue type can be utilized. | |

| | |
|---|---|
| Venue Name | Enter the venue name and address. The operator can configure an access point to describe the location of the hotspot. This information typically includes the name and address of the deployment location where the hotspot is located. Enter the name and address configured for the access point hotspot. The name cannot exceed 252 characters. |
| Venue Name Long | Hotspot operators can list venue names in multiple languages. Select the **+ Add Row** button to add venue name languages. Enter the two- or three-character ISO-14962-1997 encoded string that defines the language used in the **Code** field. Enter the name of the venue in the **Name** field. The name cannot exceed 252 characters. |

10 Refer to the **Operator Network Parameters** field to define the following:

| | |
|---|---|
| Operator Name | Provide the unique name (in English) of the administrator or operator responsible for the configuration and management or the hotspot. The name cannot exceed 64 characters. |
| Operator Name Long | Operator names can be listed in multiple languages. Select the **+ Add Row** button to add operator name languages. Enter the two- or three-character ISO-14962-1997 encoded string that defines the language used in the **Code** field. Enter the name of the operator in the **Name** field. The name cannot exceed 252 characters. |
| PLMNID | Operators providing mobile and Wi-Fi hotspot services have a unique *Public Land Mobile Network* (PLMN) ID. Select the **+ Add Row** button to add PLMN information for operators responsible for the configuration and operation of the hotspot. Provide a description for the PLMN, not exceeding 64 characters.<br>Enter a three-digit *Mobile Country Code* (MCC) and two-digit *Mobile Network Code* (MNC) for the PLMN ID. The MCC identifies the region and country where the hotspot is deployed. The MNC identifies the operator responsible for the configuration and management of the hotspot by PLMN ID and country. Both the MCC and MNC fields are mandatory. |

11 Click **OK** to update the passpoint policy settings.

Click **Reset** to revert to the last saved configuration.

12 Select **NAI Realm**.

The Network Access Identifier (NAI) is the user identity submitted by the hotspot requesting client during authentication. The standard syntax is `user@realm`. NAI is frequently used when roaming, to identify the user and assist in routing an authentication request to the user's authentication server. The realm name is often the domain name of the service provider.

The NAI Realm screen displays those realms created thus far for utilization with a passpoint policy.

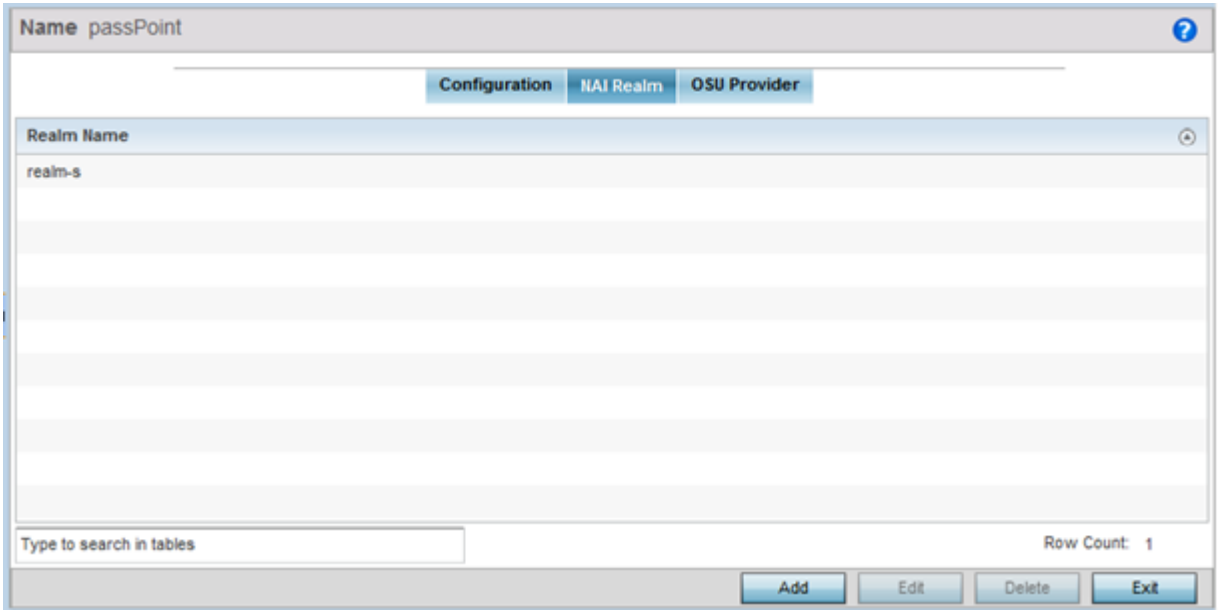



**Figure 328: Passpoint Policy - NAI Realm Screen**

13 Click **Add** to create a new NAI realm configuration for passpoint hotspot utilization, **Edit** to modify the attributes of an existing configuration, or **Delete** to remove a selected configuration from those available.

Provide a realm name or names (32 characters maximum), delimited by semicolons. Click **+ Add Row** to create an EAP Method configuration for the NAI realm.

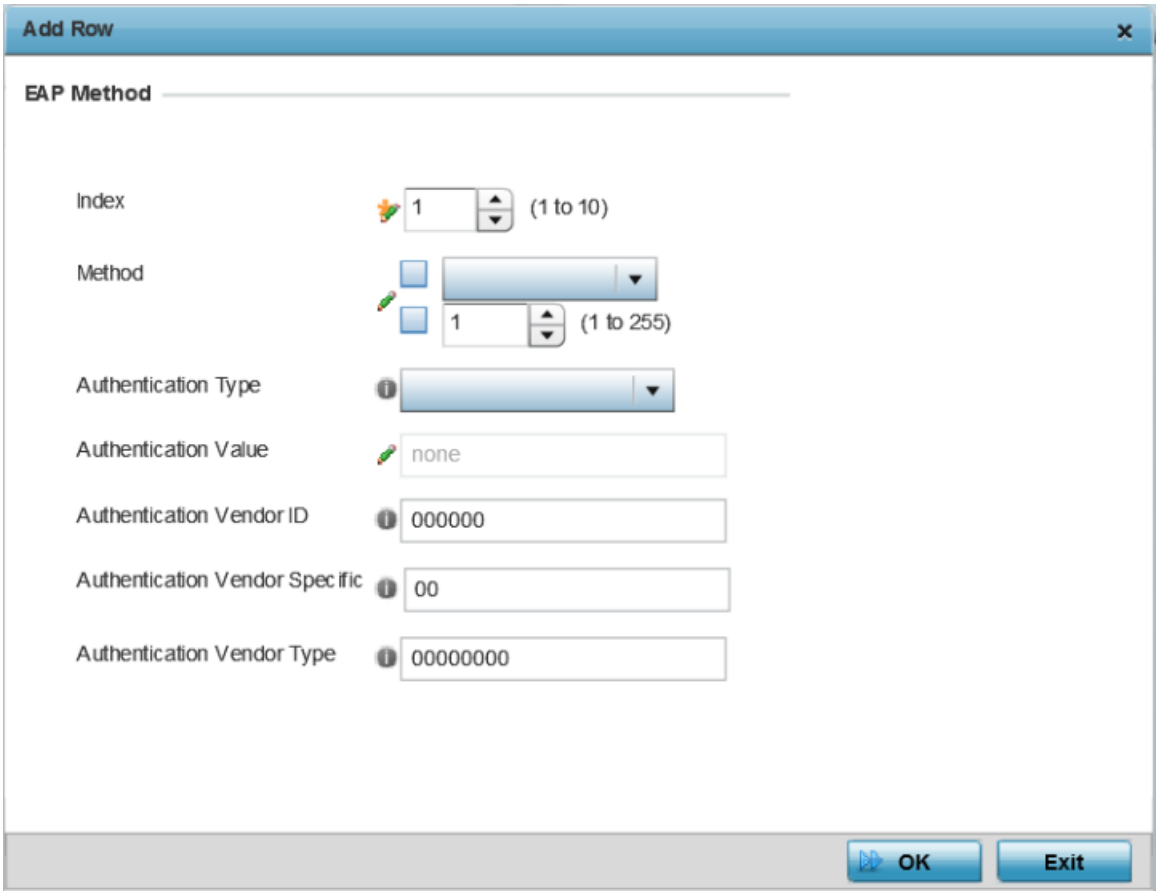



**Figure 329: Passpoint Policy - NAI Realm EAP Method Screen**

14 Set the following **EAP Method** attributes to secure the NAI realm used by the passpoint policy:

| | |
|---|---|
| Index | Select an EAP instance index from 1 - 10 to apply to this hotspot's EAP credential exchange and verification session. NAIs are often user identifiers in the EAP authentication protocol. |
| Method | Set an EAP method for the NAI realm. Options include **identity**, **otp**, **gtc**, **rsa-public-key**, **tls**, **sim**, **ttls**, **peap**, **ms-auth**, **ms-authv2**, **fast**, **psk**, and **ikev2**. |
| Authentication Type | Specify the EAP method authentication type. Options include **expanded-eap**, **non-eap-inner**, **inner-eap**, **expanded-inner-eap**, **credential**, **tunn-eap-credential**, and **vendor**. |
| Authentication Value | If you are setting the authentication type to either **non-eap-inner**, **inner-eap**, **credential**, or **tunnel-eap-credential**, define an authentication value that must be shared with the EAP credential validation server resource. |

| | |
|---|---|
| Authentication Vendor ID | If the authentication type is set to either **expanded-eap** or **expanded-inner-eap**, set a six-character authentication vendor ID. This ID must match the ID utilized by the EAP server resource. |
| Authentication Vendor Specific | If required, add 2 - 510 character vendor-specific authentication data required for the selected authentication type. Enter the value in an `a- FA -F0-9` format. |
| Authentication Vendor Type | Set an eight-character authentication vendor type used exclusively for the **expanded-eap** or **expanded-inner-eap** authentication types. |

15 Click **OK** to save the updates to the NAI realm.

Click **Reset** to revert to the last saved configuration.

16 Select **OSU Provider**.

WiNG managed clients can use *Online Sign-Up* (OSU) for registration and credential provisioning to obtain hotspot network access. Service providers have an OSU AAA server and certificate authority (CA). For a client and hotspot to trust one another, the OSU server holds a certificate signed by a CA whose root certificate is issued by a CA authorized by the Wi-Fi Alliance, and CA certificates are installed on the client device. A CA performs the following functions:

- Issues certificates (creates and signs)
- Maintains certificate status information and issues certificate revocation lists (CRLs)
- Publishes current (non-expired) certificates and CRLs
- Maintains status archives for the expired or revoked certificates it has issued

Passpoint certificates are governed by the Hotspot 2.0 OSU Certificate Policy Specification. An OSU server certificate should be obtained from any of the CAs authorized by the Wi-Fi Alliance. Once an OSU provider is selected, the client connects to the OSU WLAN. It then triggers an HTTPS connection to the OSU server, which was received with the OSU providers list. The client validates the server certificate to ensure it's a trusted OSU server. The client is prompted to complete an online registration through their browser. When the client has a valid credential for the hotspot 2.0 WLAN, it disassociates from the OSU WLAN and connects to the hotspot 2.0 WLAN.

The OSU Provider screen displays those provider configurations created thus far for use with a passpoint policy.

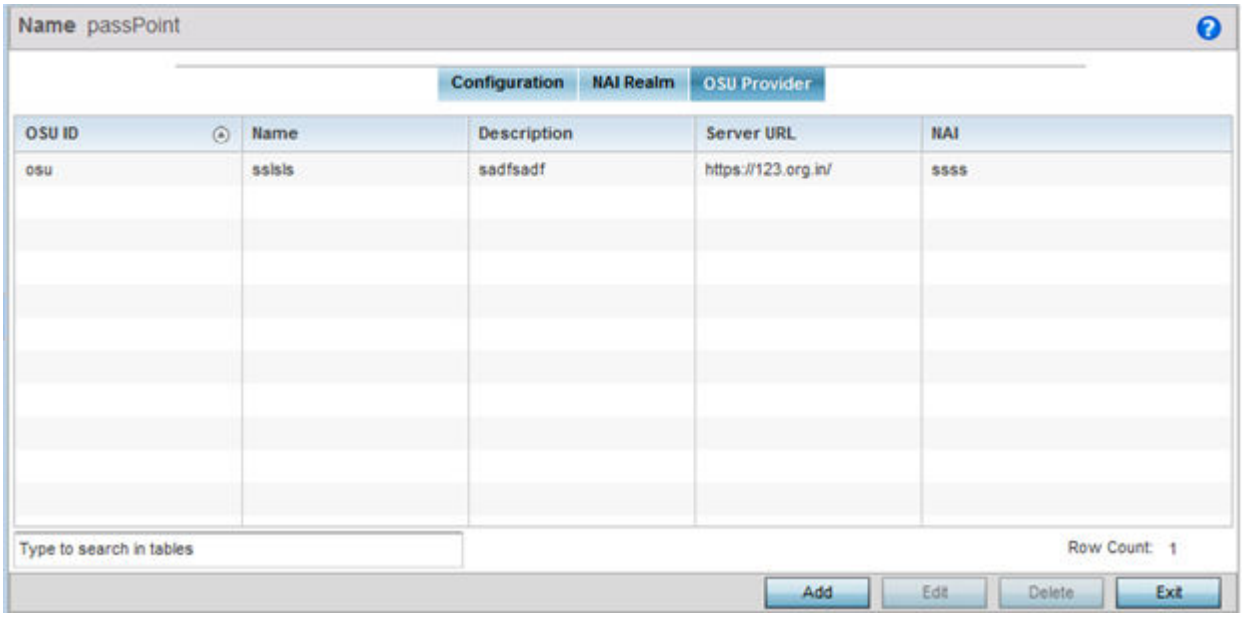



**Figure 330: Passpoint Policy - OSU Provider Screen**

17 Click **Add** to create a new OSU provider configuration for passpoint hotspot utilization, **Edit** to modify the attributes of an existing configuration, or **Delete** to remove a selected configuration from those available.

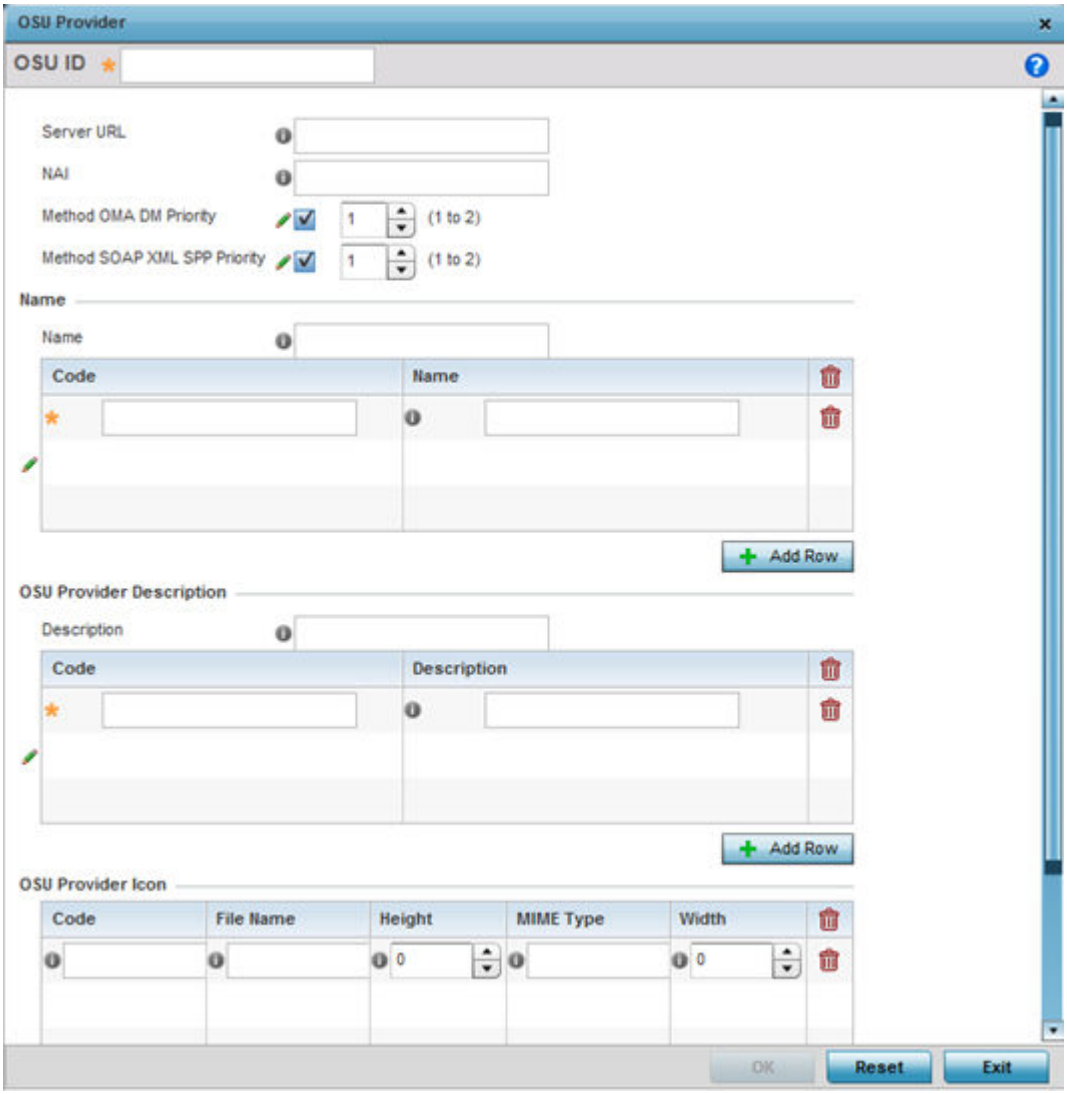



**Figure 331: Passpoint Policy - OSU Provider - Add/Edit Screen**

18 If you are creating a new OSU provider configuration, provide it a 32-character maximum OSU ID that will serve as an online sign up identifier.

19 Set the following attributes to secure the *Network Access Identifier* (NAI) submitted by the hotspot during OSU authentication:

| | |
|---|---|
| Server URL | Provide a 255 character maximum sign up server URL for the OSU provider. |
| NAI | Enter a 255 character maximum NAI to identify the user and assist in routing an authentication request to the authentication server. The realm name is often the domain name of the service provider. |

| | |
|---|---|
| Method OMA DM Priority | Select this option to provide *Open Mobile Alliance* (OMA) device management priority. OMA is a standards body developing open standards for mobile clients. OMA is relevant to service providers working across countries (with different languages), operators and mobile terminals. Adherence to OMA is strictly voluntary. Use the drop-menu to specify the priority as 1 or 2. |
| Method SOAP XML SPP Priority | Select this option to apply a SOAP-XML subscription provisioning protocol priority of either 1 or 2. The *simple object access protocol* (SOAP) is a protocol for exchanging structured information in web services. SOAP uses XML as its message format and relies on other application layer protocols, like HTTP or SMTP, for message negotiation and transmission. |

20 Refer to the **Name** field to optionally set a 252-character English language sign up name, then provide a 3-character maximum ISO-639 language code to apply the sign up name in a language other then English.

Apply a 252-character maximum hexadecimal online sign up name to encode in the ISO-639 language code applied to the sign up name.

21 Refer to the **OSU Provider Description** field to set an online sign up description in a language other then English.

Select **+ Add Row** and provide a 3-character maximum ISO-639 language code to apply the sign up name in a language other then English. Apply a 252-character maximum hexadecimal online sign up description to encode in the ISO-639 language code applied to the sign up name.

22 Optionally provide an **OSU Provider Icon** by selecting **+ Add Row**.

Apply the following configuration attributes to the icon.

| | |
|---|---|
| Code | Enter a 3-character maximum ISO-639 language Code to define the language used in the OSU provider icon. |
| File Name | Provide a 255-character maximum icon name and directory path location for the icon file. |
| Height | Provide the icon's height in pixels from 0 - 65,535. The default setting is 0. |
| MIME Type | Set the icon's MIME file type from 0 - 64. The MIME associates filename extensions with a MIME type. A MIME enables a fallback on an extension and are frequently used by web servers. |
| Width | Provide the icon's width in pixels from 0 - 65,535. The default setting is 0. |

23 Click **OK** to save the updates to the OSU Provider configuration.

Click **Reset** to revert to the last saved configuration.

## Sensor Policy

*Wireless Intrusion Protection System* (WIPS) protects wireless client and access point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

In addition to dedicated AirDefense sensors, an access point radio can function as a sensor and upload information to a dedicated WIPS server (external to the access point). Unique WIPS server configurations can be used to ensure a WIPS server configuration is available to support the unique data protection needs of an RF Domain.

WIPS is not supported on a WLAN basis. Instead, sensor functionality is supported on the access point radio(s) available to each managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all legal channels within the 2.4 and 5.0 GHz band. Sensor support requires an AirDefense WIPS server on the network. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server.

In addition to WIPS support, sensor functionality has now been added for Extreme Networks' locationing system (ExtremeLocation). The ExtremeLocation system for Wi-Fi locationing includes WiNG controllers and access points functioning as sensors. Within the ExtremeLocation architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated ExtremeLocation server resource, as opposed to an ADSP server. The ExtremeLocation server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices.

## Configuring a Sensor Policy

To define a sensor policy for use with an RF Domain:

1 Select **Configuration → Wireless → Sensor Policy** to display existing sensor policies.

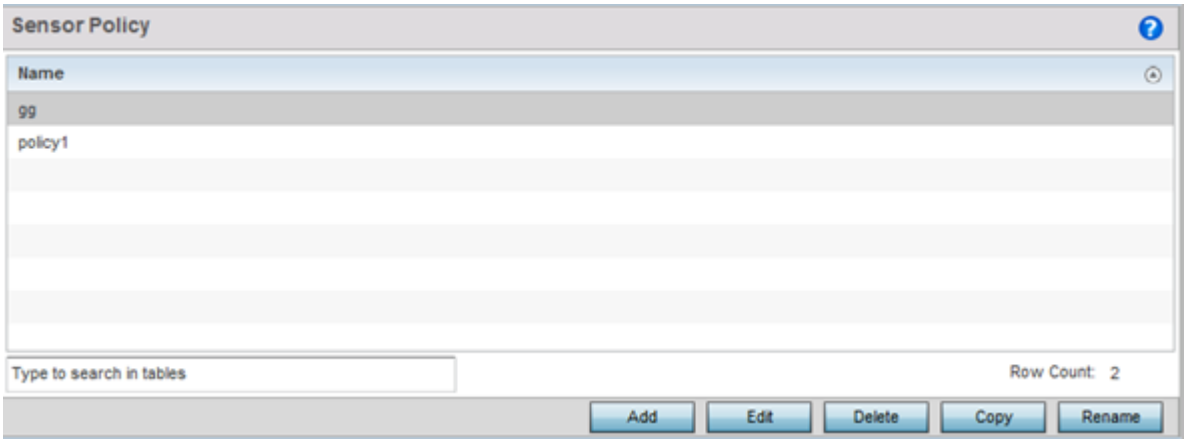



**Figure 332: Sensor Policy Screen**

2 Click **Add** to define a new sensor policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy.

Optionally, **Copy** or **Rename** sensor policies as needed.

When you are adding a new sensor policy, the Add New Sensor Policy screen displays:

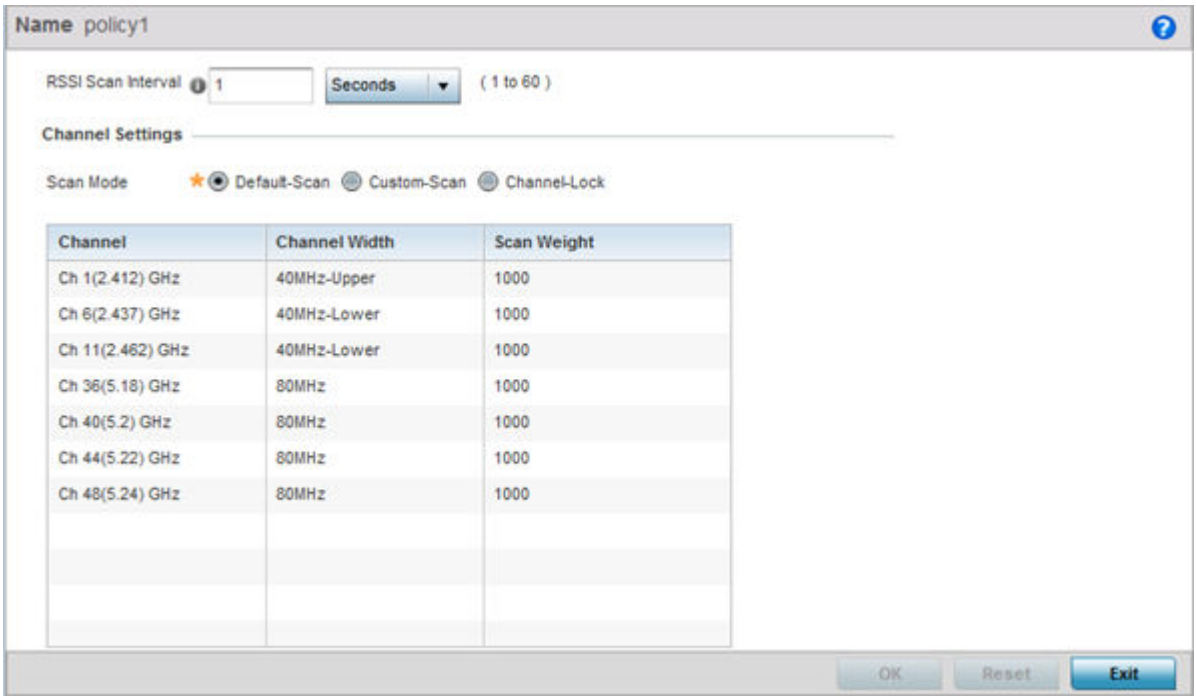



**Figure 333: Wireless - Sensor Policy - Add New Sensor Policy Screen**

3 Provide a name for this sensor policy in the **Name** field.

Sensor policy name cannot exceed 32 characters and cannot contain spaces.

4 Select **Continue** to create the sensor policy.

The Sensor Policy Addition screen displays with the **Scan Mode** set to **`Default-Scan`**. The user configurable parameters on this screen differ, depending on which **Scan Mode** is selected.

5 Use the **RSSI Scan Interval** drop-down menu to set a scan interval from 1 - 60 seconds.

This is the scan period used by dedicated sensors (access point radios) for RSSI (signal strength) assessments. Once the sensor obtains the RSSI data, the sensor sends the data to a specified ExtremeLocation server resource (not an ADSP server) for calculating Wi-Fi device locations. The default is 1 second.

6 Set the following **Scan Mode** values.

The values you can select depend on whether you have selected **`Default-Scan`**, **`Custom-Scan`**, or **`Channel-Lock`** as the mode for scan operation.

| | |
|---|---|
| Channel | With **Default-Scan** selected: The list of available scan channels is fixed and defaulted in a spread pattern of 1, 6, 11, 36, 40, 44 and 48. You cannot change this channel pattern.<br>With **Custom-Scan** selected: A list of unique channels in the 2.4, 4.9, 5 and 6 GHz band can be collectively or individually enabled for customized channel scans and RSSI reporting.<br>With **Channel-Lock** selected: The **Channel**, **Channel Width**, and **Scan Weight** fields are replaced by a **Lock Frequency** drop-down menu. Use this menu to lock the RSSI scan to one specific channel. |
| Channel Width | With **Default-Scan** selected: Each channel's width is fixed and defaulted to either 40MHz-Upper (Ch 1), 40MHz-Lower (Ch 6 and CH 11) or 80MHz (CH 36, CH 40, CH 44 and CH 48).<br>With **Custom-Scan** selected: You can define the width for each selected channel. Note that many channels have their width fixed at 20MHz. 802.11a radios support 20 and 40 MHz channel widths.<br>With **Channel-Lock** selected: You cannot adjust the width between adjacent channels, because only one channel is locked. |
| Scan Weight | With **Default-Scan** selected: Each default channel's scan is of equal duration (1000) within the defined RSSI scan interval. No one channel receives scan priority within the defined RSSI scan interval.<br>With **Custom-Scan** selected: Each selected channel can have its weight prioritized in respect to the amount of time a scan is permitted within the defined RSSI scan interval.<br>With **Channel-Lock** selected: With one channel locked for an RSSI scan, you cannot adjust scan weights for other, unlocked channels. |

7 Click **OK** to save the updates to the sensor policy configuration.

Click **Reset** to revert to the last saved configuration.

8 To create a copy of a sensor policy, select the policy and click **Copy**.

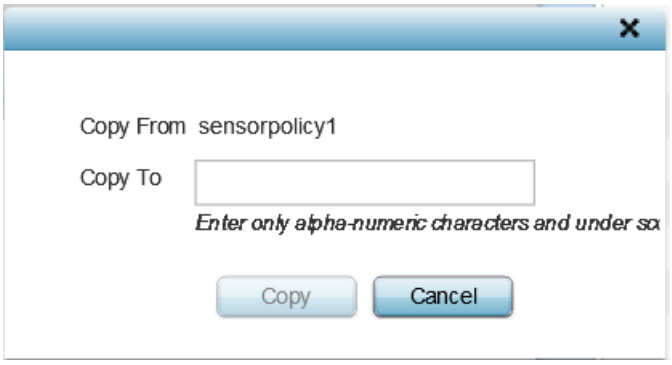



**Figure 334: Wireless - Sensor Policy - Copy Policy Screen**

Use the **Copy To** field to provide a name for the new sensor policy being created. The name of the new policy cannot be longer than 32 characters and cannot contain spaces.

9 To rename an existing sensor policy, select the policy and click **Rename**.

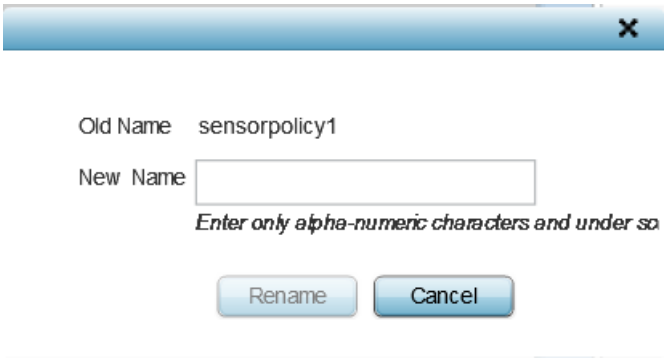



**Figure 335: Wireless - Sensor Policy - Rename Policy Screen**

Use the **New Name** field to provide a new name for the sensor policy. The new name cannot be longer than 32 characters and cannot contain spaces.

10 To delete a sensor policy, select it and click **Delete**.

This removes the policy from the list of sensor policies.

# 8 Network Configuration



Controllers, service platforms and Access Points allow packet routing customizations and unique network resources for deployment specific routing configurations.

For more information on the options available, refer to the following:



## Policy Based Routing (PBR)

Define a policy based routing (PBR) configuration to direct packets to selective paths. PBR can optionally mark traffic for preferential services. PBR minimally provides the following:

- A means to use source address, protocol, application and traffic class as traffic routing criteria
- The ability to load balance multiple WAN uplinks
- A means to selectively mark traffic for QoS optimization

Since PBR is applied to incoming routed packets, a route-map is created containing a set of filters and associated actions. Based on the actions defined in the route-map, packets are forwarded to the next relevant hop. Routemaps are configurable under a global policy called routing-policy, and applied to profiles and devices.

Route-maps contain a set of filters which select traffic (match clauses) and associated actions (set clauses) for routing. A routemap consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value). If it matches, the routing decision is based on this route-map. If the packet does not match the route-map, the route-map entry with next highest precedence is matched. If the incoming packet does not match any of the route-map entries, it's subjected to typical destination based routing. Each route-map entry can optionally enable/disable logging.

The following criteria can optionally be used as traffic selection segregation criteria:

- IP Access List - A typical IP ACL can be used for traffic permissions. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.
- IP DSCP - Packet filtering can be performed by traffic class, as determined from the IP DSCP field. One DSCP value is configurable per route map entry. If IP ACLs on a WLAN, ports or SVI mark the packet, the new/ marked DSCP value is used for matching.
- Incoming WLAN - Packets can be filtered by the incoming WLAN. There are two ways to match the WLAN:
  - If the device doing policy based routing has an onboard radio and a packet is received on a local WLAN, then this WLAN is used for selection.
  - If the device doing policy based routing does not have an onboard radio and a packet is received from an extended VLAN, then the device which received the packet passes the WLAN information in the MINT packet for the PBR router to use as match criteria.
- Client role - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
- Incoming SVI - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the host originating the packet is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing policy based routing, and not the originating connected device.

Each route map entry has a set of match and set (action) clauses. ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

Set (or action) clauses determine the routing function when a packet satisfies match criteria. If no set clauses are defined, the default is to fallback to destination based routing for packets satisfying the match criteria. If no set clause is configured and fallback to destination based routing is disabled, then the packet is dropped. The following can be defined within set clauses:

- Next hop - The IP address of the next hop or the outgoing interface through which the packet should be routed. Up to two next hops can be specified. The outgoing interface should be a PPP, a

tunnel interface or a SVI which has DHCP client configured. The first reachable hop should be used, but if all the next hops aren't reachable, typical destination based route lookup is performed.

- Default next hop - If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This can be either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reversed. With both cases:
  - If a defined next hop is reachable, it's used. If fallback is configured refer to (b).
  - Do normal destination based route lookup. If a next hop is found its used, if not refer to (c).
  - If default next hop is configured and reachable, it's used. If not, drop the packet.
- Fallback - Fallback to destination based routing if none of the configured next hops are reachable (or not configured). This is enabled by default.
- Mark IP DSCP - Set IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

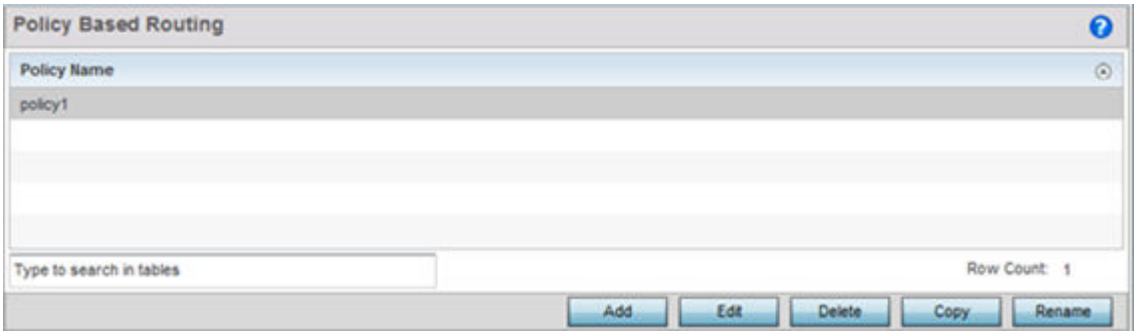
Note

A packet should optimally satisfy all the match criteria, if no match clause is defined in a route-map, it would match everything. Packets not conforming to any of the match clauses are subjected to normal destination based routing.

To define a PBR configuration:

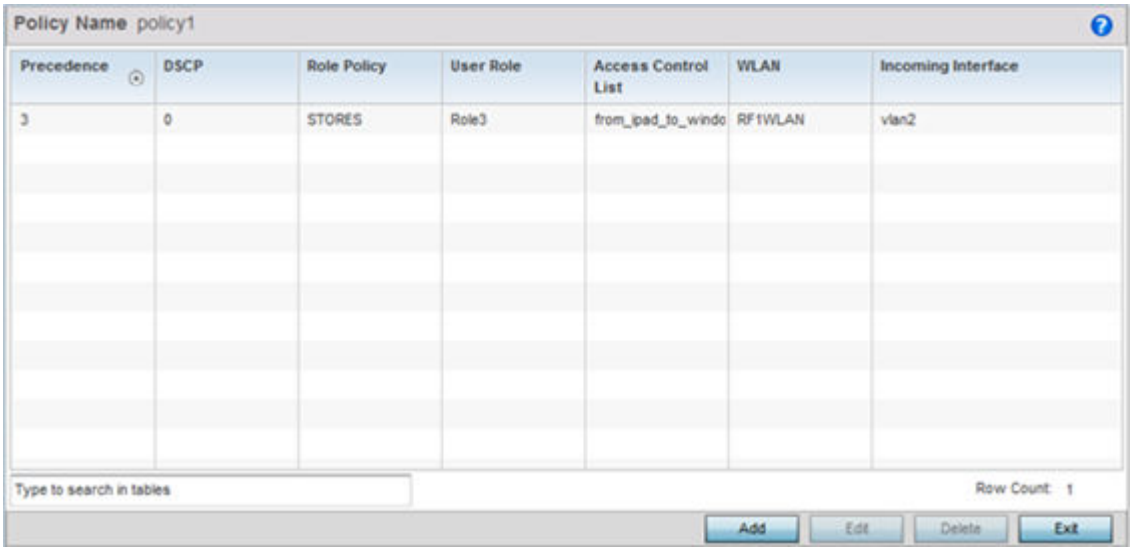
1 Select **Configuration → Network → Policy Based Routing**.

The Policy Based Routing screen displays.




2 Select **Add** to create a new PBR configuration, **Edit** to modify the attributes of an existing PBR configuration, or **Delete** to remove a selected PBR configuration. Select **Copy** to copy the selected PBR configuration or **Rename** to rename the PBR configuration.

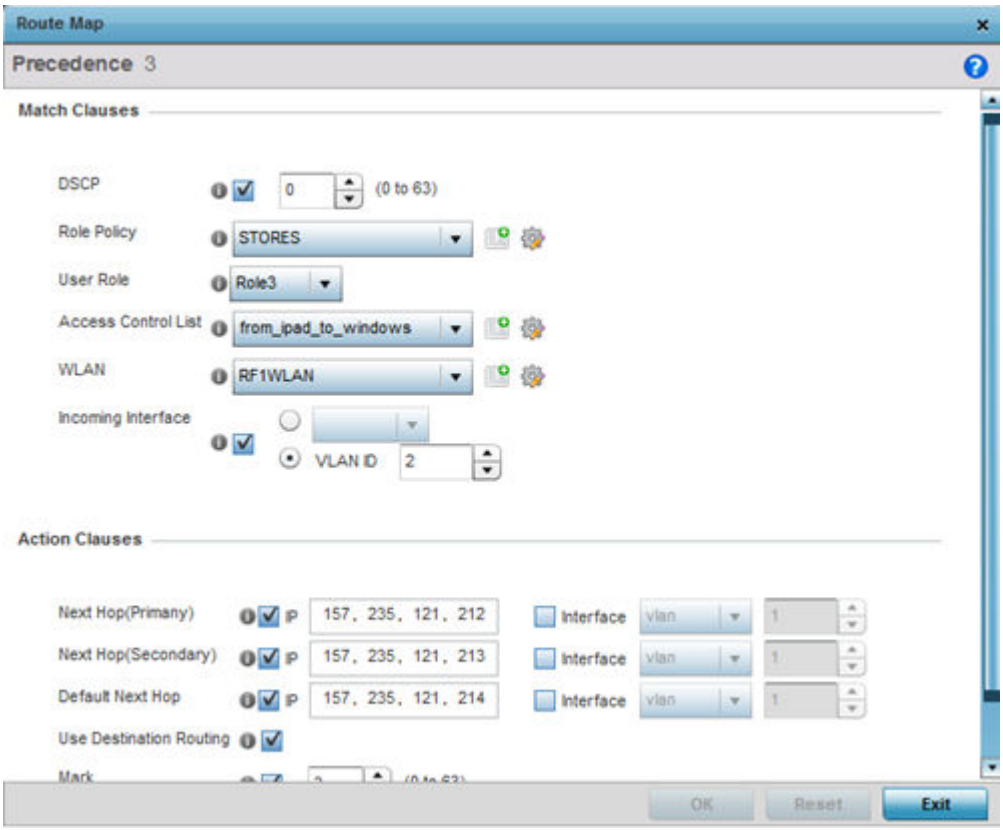
3 If creating a new PBR policy assign it a Policy **Name** up to 32 characters to distinguish this route map configuration from others with similar attributes. Select **Continue** to proceed to the Policy Name screen where route map configurations can be added, modified or removed. Select **Exit** to exit without creating a PBR policy.




4 Refer to the following to determine whether a new route-map configuration requires creation or an existing route-map requires modification or removal:

| | |
|---|---|
| Precedence | Lists the numeric precedence (priority) assigned to each listed PBR configuration. A routemap consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value). |
| DSCP | Displays each policy's DSCP value used as matching criteria for the route map. DSCP is the Differentiated Services Code Point field in an IP header and is for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. One DSCP value can be configured per route map entry. |
| Role Policy | Lists each policy's role policy used as matching criteria. |
| User Role | Lists the user role defined in the Role Policy. |
| Access Control List | Displays each policy's IP ACL used as an access/deny filter criteria for the route map. |
| WLAN | Displays each policy's WLAN used as an access/deny filter for the route map. |
| Incoming Interface | Display the name of the Access Point WWAN or VLAN interface on which the packet is received for the listed PBR policy. |

5 Select **Add** or **Edit** to create or modify a route-map configuration. Configurations can optionally be removed by selecting **Delete**.




6 If adding a route map, use the spinner control to set a numeric Precedence (priority) for this route-map. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value).

7 Refer to the Match Clauses field to define the following matching criteria for the route-map configuration:

| | |
|---|---|
| DSCP | Select this option to enable a spinner control to define the DSCP value used as matching criteria for the route map. DSCP is the Differentiated Services Code Point field in an IP header and is for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. One DSCP value can be configured per route map entry. |
| Role Policy | Use the drop-down to select a Role Policy to use with this route-map. Click the Create icon to create a new Role Policy. To view and modify an existing policy, click the Edit icon. |
| User Role | Use the drop-down menu to select a role defined in the selected Role Policy. This user role is used while deciding the routing. |
| Access Control List | Use the drop-down menu to select an IP based ACL used as matching criteria for this route-map. Click the Create icon to create a new ACL. To view and modify an existing ACL, click the Edit icon. |

| | |
|---|---|
| WLAN | Use the drop-down menu to select the Access Point WLAN used as matching criteria for this route-map. Click the Create icon to create a new WLAN. To view and modify an existing WLAN, click the Edit icon. |
| Incoming Interface | Select this option to enable radio buttons used to define the interfaces required to receive route-map packets. Use the drop-down menu to define either the Access Point's wwan1 or pppoe1 interface. Neither is selected by default. Or, select the VLAN ID option to define the Access Point VLAN to receive route-map-packets. |

8 Set the following **Action Clauses** to determine the routing function performed when a packet satisfies match criteria. Optionally fallback to destination based routing if no hop resource is available.

| | |
|---|---|
| Next Hop (Primary) | Define a first hop priority request. Set either the IP address of the virtual resource or select the Interface option and define either a wwan1, pppoe1 or a VLAN interface. In the simplest terms, if this primary hop resource is available, its used with no additional considerations. |
| Next Hop (Secondary) | If the primary hop request were unavailable, a second resource can be defined. Set either the IP address of the virtual resource or select the Interface option and define either a wwan1, pppoe1 or a VLAN interface. |
| Default Next Hop | If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This value is set as either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reverse. Set either the next hop IP address or define either a wwan1, pppoe1 or a VLAN interface. |
| Use Destination Routing | It may be a good idea to select this option to default back to destination based routing if none of the defined hop resources are reachable. Packets are dropped if a next hop resource is unavailable and fallback to destination routing is disabled. This option is enabled by default. |
| Mark | Select this option and use the spinner control to set IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL. |

9 Select **OK** to save the updates to the route-map configuration. Select **Reset** to revert to the last saved configuration.

## L2TP V3 Configuration

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network. L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables WiNG supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WiNG managed devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. WiNG managed access points support an Ethernet VLAN pseudowire type exclusively.

**Note**
A pseudowire is an emulation of a layer 2 point-to-point connection over a PSN *(packet-switching network)*. A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

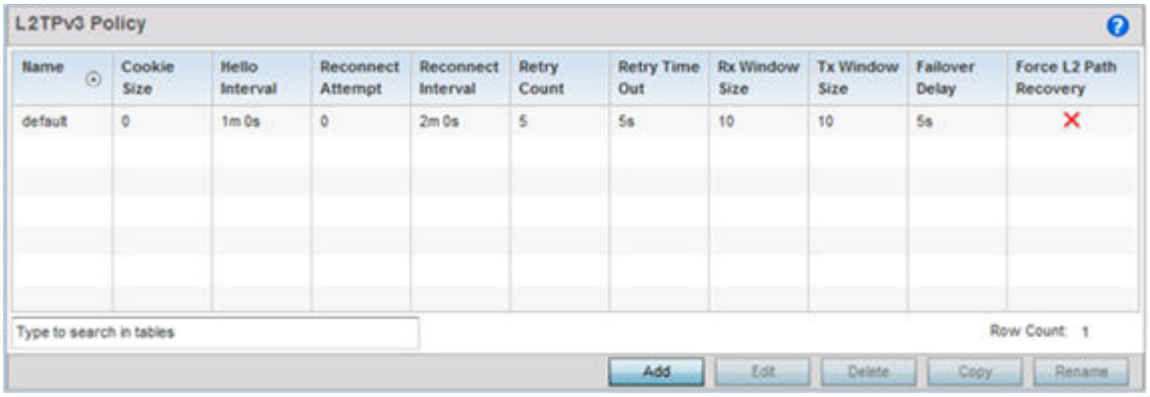
The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

**Note**
If connecting an Ethernet port to another Ethernet port, the pseudowire type must be Ethernet port, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be Ethernet VLAN.

To define an L2TP V3 tunnel configuration:

1 Select **Configuration → Network → L2TP V3**.

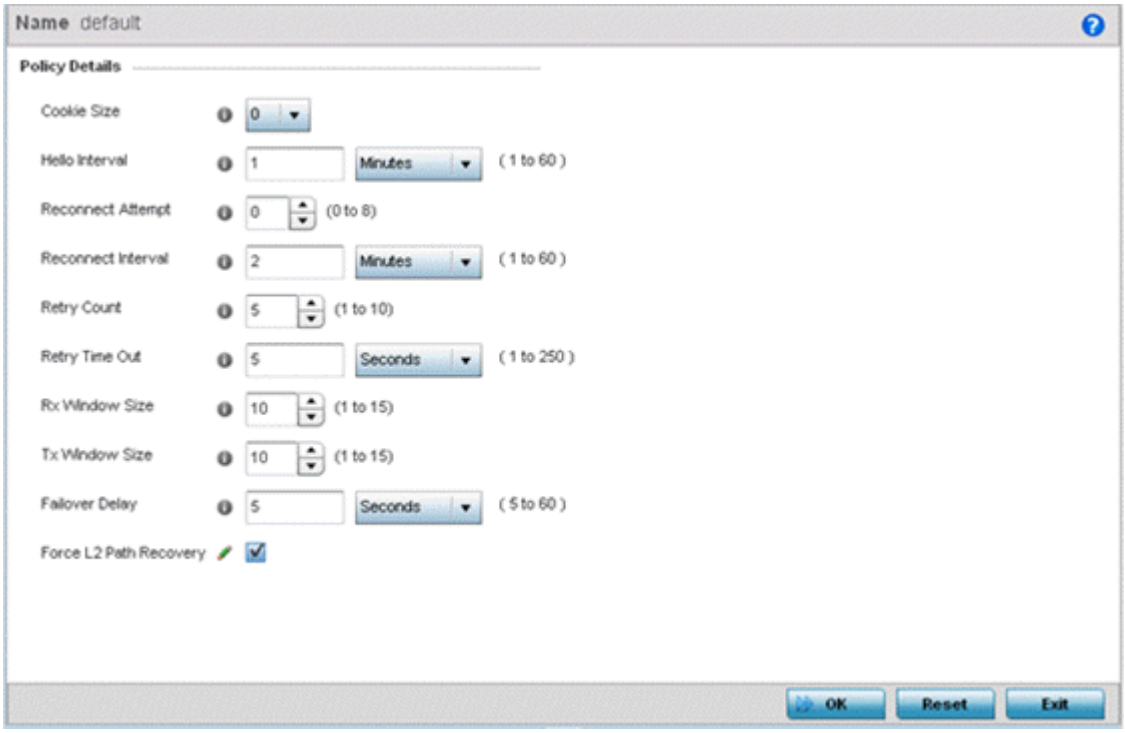
The L2TP V3 screen opens and lists the policy configurations defined thus far.



2 Refer to the following to determine whether a new L2TP V3 requires creation or modification:

| | |
|---|---|
| Name | Lists the 31 character maximum name assigned to each listed L2TP V3 policy upon creation. |
| Cookie size | Displays the size of each policy's cookie field within each L2TP V3 data packet. L2TP V3 data packets contain a session cookie which identifies the session (pseudowire) corresponding to it. If using the CLI, the cookie size can't be configured per session, and are the same size for all sessions with in a tunnel. |
| Hello Interval | Displays each policy's interval between L2TP V3 hello keep alive messages exchanged within the L2TP V3 connection. |
| Reconnect Attempts | Lists each policy's maximum number of re-connection attempts to reestablish a tunnel between peers. |
| Reconnect Interval | Displays the duration set for each listed policy between two successive reconnection attempts. |
| Retry Count | Lists the number of retransmission attempts set for each listed policy before a target tunnel peer is defined as not reachable. |
| Retry Time Out | Lists the interval the interval (in seconds) set for each listed policy before the retransmission of a L2TP V3 signaling message. |
| Rx Window Size | Displays the number of packets that can be received without sending an acknowledgement. |
| Tx Window Size | Displays the number of packets that can be transmitted without receiving an acknowledgement. |
| Failover Delay | Lists the time (in either seconds or minutes) for establishing a tunnel after a failover (VRRP/RF Domain/Cluster). |
| Force L2 Path Recovery | Lists whether force L2 path recovery is enabled (as defined by a green checkmark) or disabled (as defined by a red X). Once a tunnel is established, enabling this setting forces server and gateway learning behind the L2TPv3 tunnel. |

3 Select **Add** to create a new L2TP V3 policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Select **Copy** to copy the selected L2TPv3 policy or **Rename** to rename the L2TPv3 policy.




4 If creating a new L2TP V3 policy assign it a **Name** up to 31 characters. Remember, a single L2TP V3 policy can be used by numerous L2TP V3 tunnels.

5 Define the following Policy Details to add a device to a list of devices sanctioned for network operation:

| | |
|---|---|
| Cookie size | L2TP V3 data packets contain a session cookie which identifies the session (pseudowire) corresponding to it. Use the spinner control to set the size of the cookie field present within each L2TP V3 data packet. Options include 0, 4 and 8. The default setting is 0. If using the CLI, the cookie size can't be configured per session, and are the same size for all sessions with in a tunnel. |
| Hello Interval | Define an interval in *Seconds* (1 - 3,600), *Minutes* (1 -60) or *Hours* (1) between L2TP V3 hello keep alive messages exchanged within the L2TP V3 control connection. The default setting is 1 minute. |
| Reconnect Attempts | Use the spinner control to set a value (from 0 - 250) representing the maximum number of reconnection attempts to reestablish the tunnel. The default interval is 0. |
| Reconnect Interval | Define an interval in either *Seconds* (1 - 3,600), *Minutes* (1 -60) or *Hours* (1) between two successive reconnection attempts. The default setting is 2 minutes. |
| Retry Count | Use the spinner control to define how many retransmission attempts are made before determining a target tunnel peer is not reachable. The available range is from 1 - 10, with a default value of 5. |
| Retry Time Out | Use the spinner control to set the interval (in seconds) before initiating the retransmission of a L2TP V3 signaling message. The range is from 1 - 250, with a default of 5. |
| Rx Window Size | Specify the number of packets received without sending an acknowledgment. The range is from 1 - 15, with a default of 10. |

| | |
|---|---|
| Tx Window Size | Specify the number of packets transmitted without receiving an acknowledgment. The range is from 1 - 15, with a default of 10. |
| Failover Delay | Set the time in *Seconds* (5 - 60) or *Minutes* (1) for establishing a tunnel after a failover (VRRP/RF Domain/Cluster). The default is 5 seconds |
| Force L2 Path Recovery | Determine whether force L2 path recovery is *enabled* or *disabled*. Once a tunnel is established, enabling this setting forces server and gateway learning behind the L2TPv3 tunnel. The default setting is disabled. |

6 Select **OK** to save the updates to the L2TP V3 policy. Select **Reset** to revert to the last saved configuration.

## Crypto CMP Policy

CMP *(Certificate Management Protocol)* is an Internet protocol to obtain and manage digital certificates in a PKI *(Public Key Infrastructure)* network. A CA *(Certificate Authority)* issues the certificates using the defined CMP.

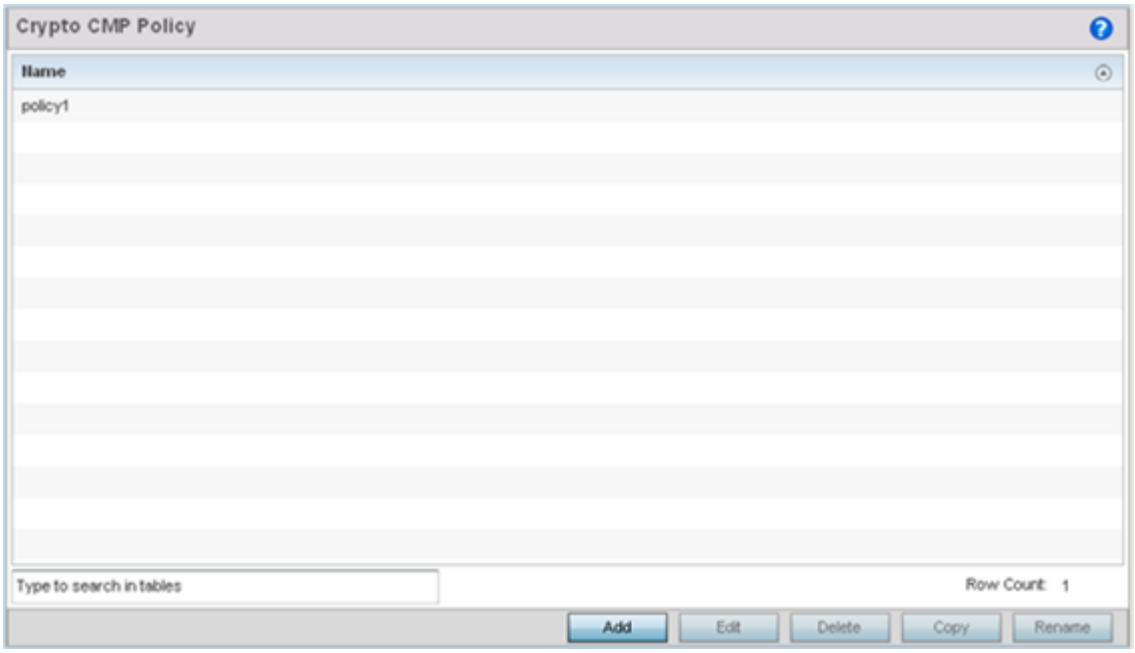
Using CMP, a device can communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.

The CMP client on the controller, service platform or Access Point triggers a request for the configured CMS CA server. Once the certificate is validated and confirmed from the CA server it is saved on the device and becomes part of the trustpoint. During the creation of the CMP policy the trustpoint is assigned a name and client information. An administrator can use a manually created trustpoint for one service (like HTTPs) and use the CMP generated trustpoint for RADIUS EAP certificate based authentication.

To review, create or edit a Crypto CMP policy:

1 Select **Configuration** → **Network**→ **Crypto CMP Policy**.

The Crypto CMP Policy screen lists the policy configuration defined thus far.



2 Select **Add** to create a new Crypto CMP policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed.

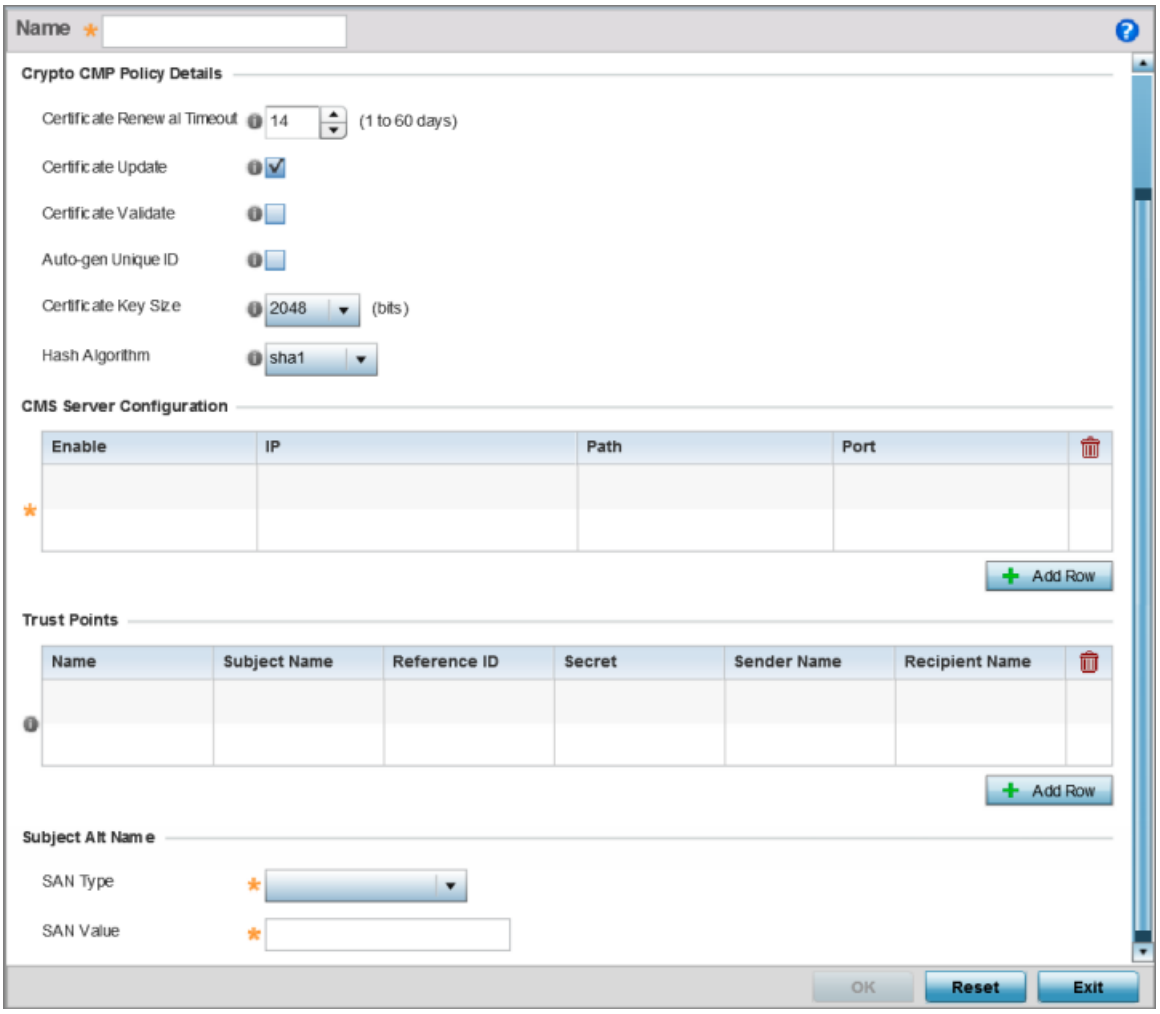



**Figure 336: Crypto CMP Policy Creation Screen**

3 If creating a new Crypto CMP policy assign it a **Name** up to 31 characters to help distinguish it.

4 Set the **Certificate Renewal Timeout** period to trigger a new certificate renewal request with the dedicated CMP server resource. The range is 1-60 days. The default is 14 days.

The expiration of the certificate is checked once a day. When a certificate is about to expire a certificate renewal is initiated with the server via an existing IPsec tunnel. If the tunnel is not established, the CMP renewal request is not sent. If a renewal succeeds the newly obtained certificate overwrites an existing certificate. If the renewal fails, an error is logged.

5 Select **Certificate Update** to update the renewal data of the certificate. This setting is enabled by default.

6 Select **Certificate Validate** to automatically validate the cross certificate with the factory certificate.

7 Select **Auto-gen Unique ID** to prepend the device's auto-generated unique ID in the subject and sender fields

8 Set the **Certificate Key Size** value. Set a value in the range 2,048 - 4,096 bits. The default value is 2048 bits. The larger the key size, the more secure the certificate.

9 Use the **Hash Algorithm** drop-down menu, to set the hashing algorithm as **`sha1`**, **`sha256`**, **`sha384`** or **`sha512`**. Hashing algorithms are mathematical functions that convert a string of characters (of indefinite length) to a fixed numerical value, much smaller than the original string. Hashing algorithms are used to sign digital certificates. The hash-algorithm type configured here is sent, in the request for certification (new or renewal), to the CA server. The CA uses the hash algorithm specified here to sign the digital certificate. The default setting is sha1.

The sha256, sha384 and sha512 hash functions belong to the SHA-2 family of algorithms.

10 Select **+ Add Row** and define the following CMS Server Configuration settings for the server resource:

| | |
|---|---|
| Enable | Use the drop-down menu to set the CMS server as either the Primary (first choice) or Secondary (secondary option) CMP server resource. |
| IP | Define the IP address for the CMP CA server managing digital certificate requests. CMP certificates are encrypted with CA's public key and transmitted to the defined IP destination over a typical HTTP or TLS session. |
| Path | Provide a complete path to the CMP CA's trustpoint. |
| Port | Provide a CMP CA port number. |

11 Set the following **Trust Points** settings. Use the **+ Add Row** button to add a row to this table. The trustpoint is used for various services as specifically set the controller, service platform or access point.

| | |
|---|---|
| Name | Enter the 32 character maximum name assigned to the target trustpoint. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. This field is mandatory. |
| Subject Name | Provide a subject name of up to 512 characters for the certificate template example. This field is mandatory. |
| Reference ID | Set the user reference value for the CMP CA trust point message. The range is 0-256. This field is mandatory. |
| Secret | Specify the secret used for trustpoint authentication over the designated CMP server resource. |
| Sender Name | Enter a sender name up to 512 characters for the trustpoint request. This field is mandatory. |
| Recipient Name | Enter a recipient name value of up to 512 characters for the trustpoint request. |

12 Set the following Subject Alt Name settings:

| | |
|---|---|
| SAN Type | Use the drop-down menu to set the Subject Alt Name type as either IP Address, Distinguished Name, Email, String, or FQDN. This field is mandatory. |
| SAN Value | Provide a Subject Alt Name value of up to 128 characters for the certificate template example. The value provided depends on the Subject Alt Name type selected. This field is mandatory. |

13 Select **OK** to save the updates to the Crypto CMP policy, **Reset** to revert to the last saved configuration, or **Exit** to close the screen.

## AAA Policy

AAA *(Authentication, Authorization, and Accounting)* provides the mechanism network administrators define access control within the network.

A controller, service platform or access point can interoperate with external RADIUS and LDAP Servers (AAA Servers) to provide an additonal user database and authentication resource. Each WLAN can maintain its own unique AAA configuration.

AAA provides a modular way of performing the following services:

*Authentication* — Authentication provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

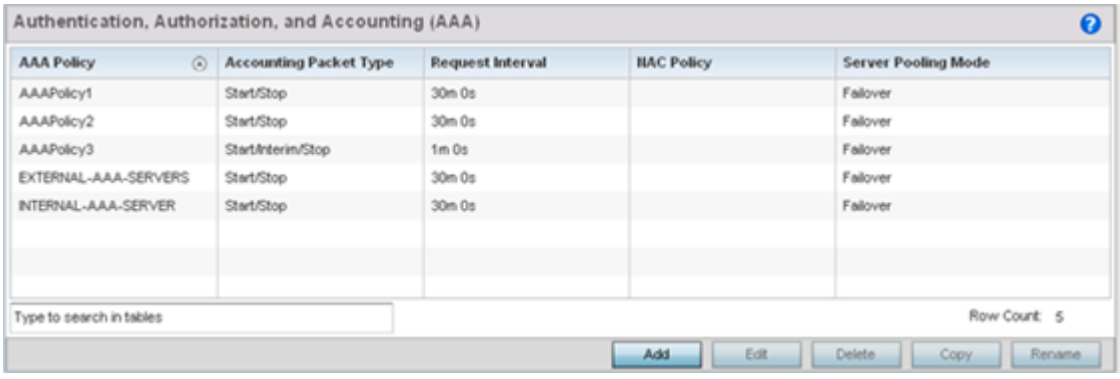
*Authorization* — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating *attribute-value* (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

*Accounting* — Accounting is the method for collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it's applied equally to all interfaces on the access servers.

To define unique controller, service platform or access point WLAN AAA configurations:

1 Select **Configuration → Network → AAA Policy**.

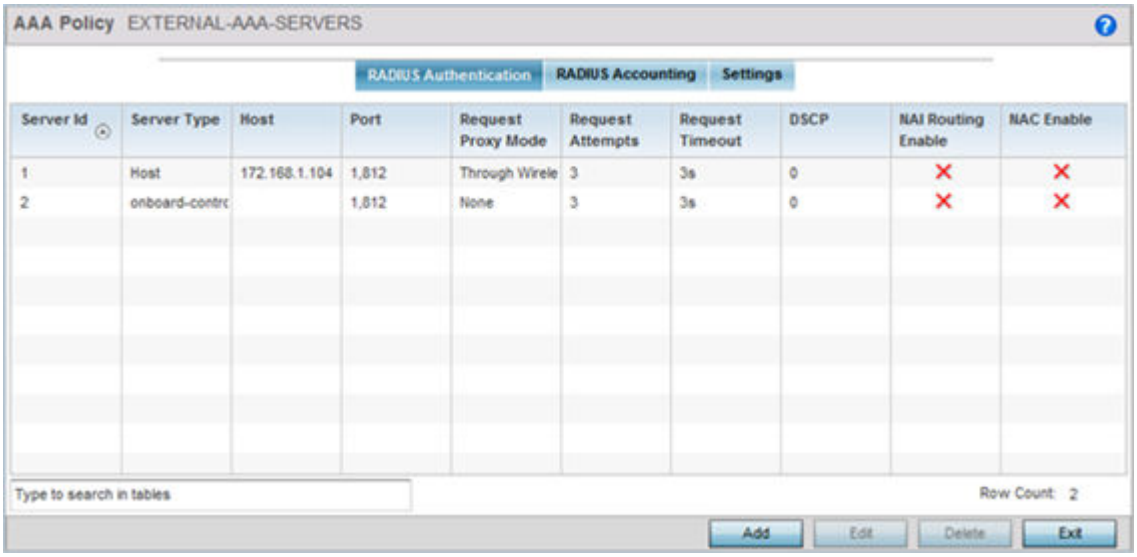
The Authentication, Authorization, and Accounting (AAA) screen displays. This screen lists AAA policies created thus far. Any of these policies can be selected and applied.



2 Refer to the following information listed for each existing AAA policy:

| | |
|---|---|
| AAA Policy | Displays the name assigned to the AAA policy when it was initially created. The name cannot be edited within a listed profile. |
| Accounting Packet Type | Displays the accounting type set for the AAA policy. Options include:<br>• *Start Only* — Sends a start accounting notice to initiate user accounting.<br>• *Start/Stop* — Sends a start accounting notice at the beginning of a process and a stop notice at the end of a process. The start accounting record is sent in the background. The requested process begins regardless of whether the start accounting notice is received by the accounting server. |
| Request Interval | Lists each AAA policy's interval used to send a RADIUS accounting request to the RADIUS server. |
| NAC Policy | Lists the name *Network Access Control* (NAC) filter used to either include or exclude clients from access. |
| Server Pooling Mode | The server pooling mode controls how requests are transmitted across RADIUS servers. Selecting **`Failover`** results in working down the list of servers if a server is unresponsive and unavailable. The **`Load Balanced`** option uses all available servers transmitting requests in round robin. |

3 To configure a new AAA policy, click **Add**. To modify an existing AAA configuration, select it from amongst those available and click **Edit**. Existing policies can be copied or renamed as needed.

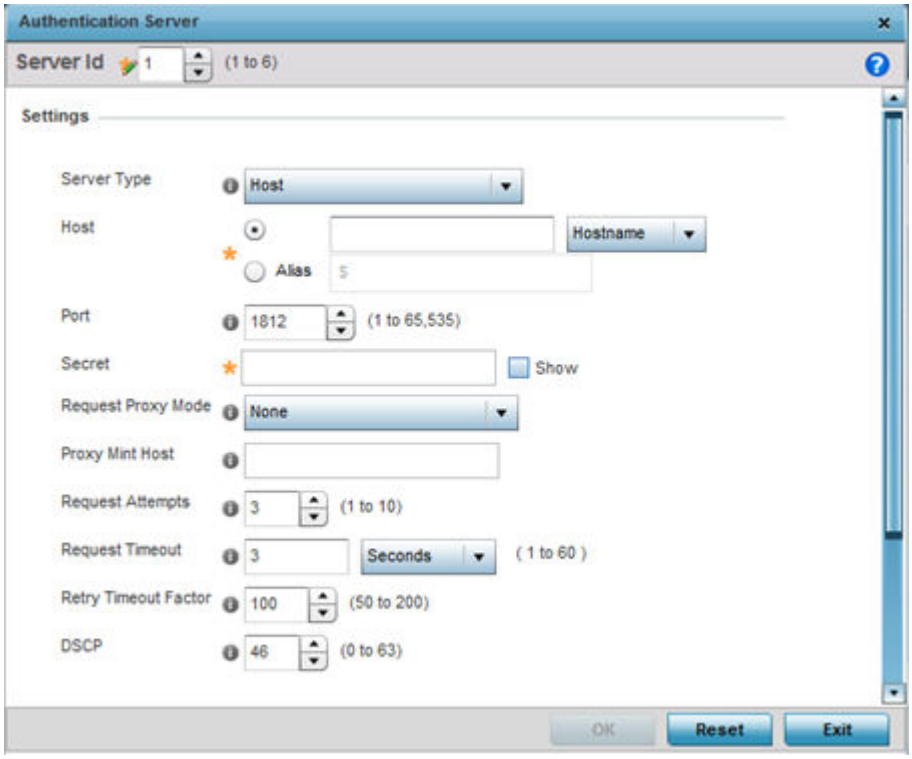



4 Refer to the following RADIUS Authentication details:

| | |
|---|---|
| Server Id | Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point. |
| Server Type | Displays the type of AAA server in use as either Host, onboard-self or onboard-controller. |
| Host | Displays the IP address or hostname of the RADIUS authentication server. |
| Port | Displays the port on which the RADIUS server listens to traffic within the access point managed network. The port range is 1 - 65,535. The default port is 1812. |
| Request Proxy Mode | Displays whether a request is transmitted directly through the server or proxied through the Virtual Controller AP or RF Domain manager. |

| | |
|---|---|
| Request Attempts | Displays the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3. |
| Request Timeout | Displays the time (from 1 - 60) seconds for the re-transmission of request packets. The default is 3 seconds. If this time is exceeded, the authentication session is terminated. |
| DSCP | Displays the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is from 0 - 63 with a default of 46. |
| NAI Routing Enable | Displays NAI routing status. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each. |
| NAC Enable | A green check defines NAC as enabled, while a Red X defines NAC disabled with this AAA policy. |

5 Select a configuration from the table and select **Edit**, or select **Add** to create a new RADIUS authentication server configuration. Optionally **Delete** a configuration as they become obsolete.



6 Define the following settings to add or modify AAA RADIUS authentication server configuration:

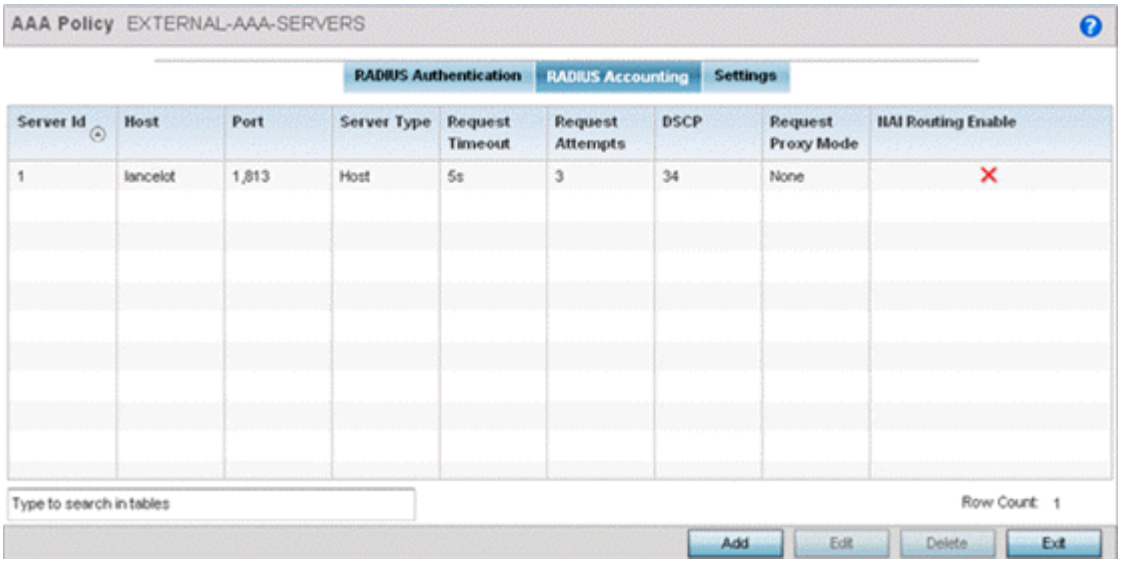
| | |
|---|---|
| Server Id | Define the numerical server index (1-6) for the authentication server to differentiate it from others available to the access point's AAA policy. |
| Server Type | Select the type of AAA server as either **Host**, **onboard-self** , **onboard-controller** or **onboard-centralized-controller**. AP 6521 model does not have an onboard authentication resource and must use an external server or Virtual Controller AP resource. |
| Host | Specify the IP address or hostname of the RADIUS authentication server. Hostnames cannot include an underscore character. Select **Alias** to define the hostname alias once and use the alias character set across different configuration items. |
| Port | Define or edit the port on which the RADIUS server listens to traffic within then access point managed network. The port range is 1 to 65,535. The default port is 1812. |
| Secret | Specify the secret used for authentication on the selected RADIUS server. By default the secret will be displayed as asterisks. To show the secret in plain text, check the **Show** box. |
| Request Proxy Mode | Select the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be **None**, **Through Wireless Controller**, **through-centralized-controller**, **Through RF Domain Manager**, or **Through Mint Host**. |
| Proxy Mint Host | Specify a 64 character maximum hostname (or Mint ID) of the Mint device used for proxying requests. Hostnames cannot include an underscore character. |
| Request Attempts | Specify the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3. |
| Request Timeout | Specify the time from 1 - 60 seconds for the access point's re-transmission of request packets. If this time is exceeded, the authentication session is terminated. The default is 3 seconds. |
| Request Timeout Factor | Specify the time from 50 - 200 seconds between retry timeouts for the access points's re-transmission of request packets. The default is 100. |
| DSCP | Specify the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is between 0 and 63 with a default value of 46. |

7 Set the following Network Access Identifier Routingvalues:

| | |
|---|---|
| NAI Routing Enable | Select this check box to enable NAI routing. AAA servers identify clients using the NAI. The NAI is a character string in the format of an E-mail address as either user or user@ but it need not be a valid E-mail address or a fully qualified domain name. NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each user credential. |
| Realm | Enter the realm name in the field. The name cannot exceed 64 characters. When the access point RADIUS server receives a request for a user name the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server. |
| Realm Type | Specify the type of realm that is being used, either Prefix or Suffix. |
| Strip Realm | Select this option to remove information from the packet when NAI routing is enabled. |

8 Select **Ok** to save the changes made to this window. Click **Exit** to close this window.

9 Select the **RADIUS Accounting** tab.

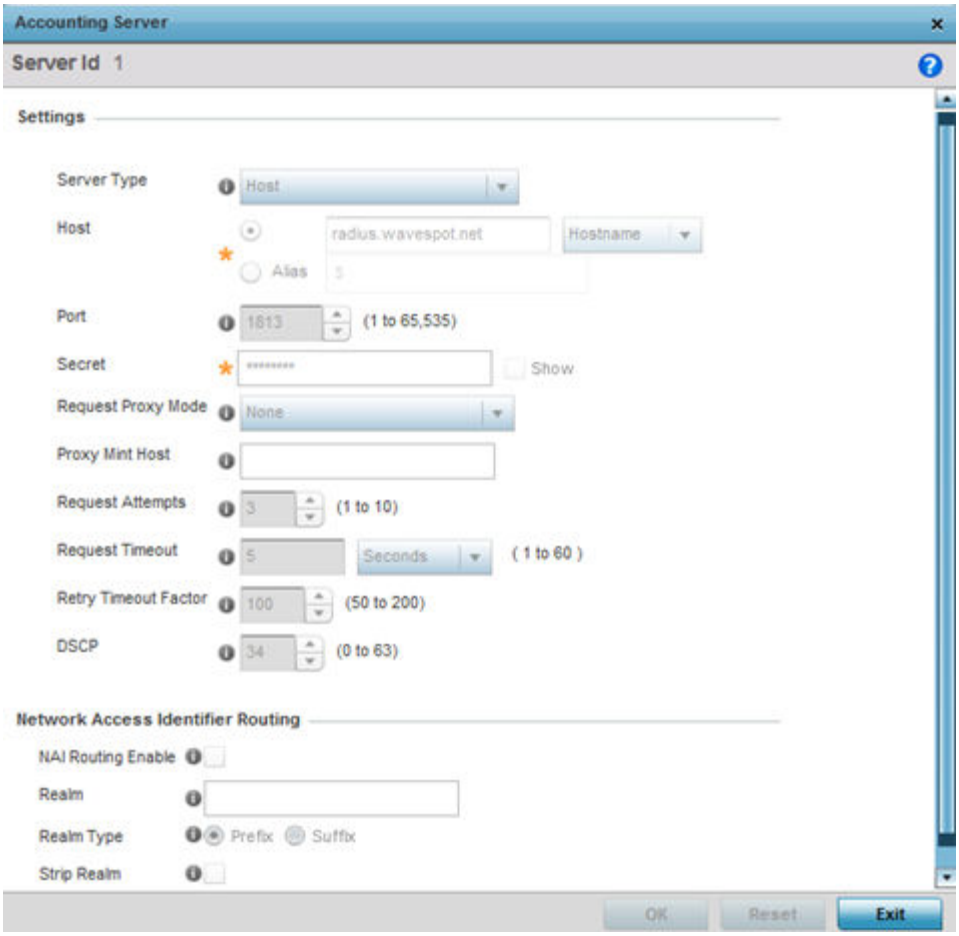



10 Refer to the following information for each existing AAA server policy to determine whether new RADIUS accounting policies require creation or existing policies require modification:

| | |
|---|---|
| Server Id | Displays the numerical server index (1-6) for the accounting server assigned when added to the WiNG operating system. |
| Host | Displays the IP address or hostname of the RADIUS authentication server. Hostnames cannot include an underscore character. |
| Port | Displays the port on which the RADIUS server listens to traffic within the network. The port range is 1 to 65,535. The default port is 1813. |
| Server Type | Displays the type of AAA server in use either Host, onboard-self, or onboard-controller. |

| | |
|---|---|
| Request Attempts | Displays the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is between 1 and 10 attempts. The default is 3 attempts. |
| Request Timeout | Displays the time between 1 and 60 seconds for the wireless controller's re-transmission of request packets. If this time is exceeded, the authentication session is terminated. |
| DSCP | Displays the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is between 0 and 63 with a default value of 34. |
| Request Proxy Mode | Displays the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be None, Through Wireless Controller, or Through RF Domain Manager. |
| NAI Routing Enable | Displays NAI routing status. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each. |

11 To edit an existing accounting profile, select the profile then **Edit**. To add a new Accounting server confguration select **Add**. Optionally **Delete** a configuration as they become obsolete.




12 Define the following settings to add or modify AAA RADIUS accounting server configuration:

| | |
|---|---|
| Server Id | Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point. |
| Host | Specify the IP address or hostname of the RADIUS accounting server. Hostnames cannot include an underscore character. Select **Alias** to define the hostname alias once and use the alias character set across different configuration items. |
| Server Type | Define or edit the port on which the RADIUS accounting server listens to traffic within the network. The port range is 1 to 65,535. The default port is 1813. |
| Secret | Specify the secret (password) used for authentication on the selected RADIUS server. By default the secret is displayed as asterisks. Select the **Show** option to display the entered secret. |
| Request Proxy Mode | Select the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be **None**, **Through Wireless Controller** , **Through RF Domain Manager** ot **Through Mint Host**. |
| Proxy Mint Host | Specify a 64 character maximum hostname or the Mint ID of the Mint device used for proxying requests. |

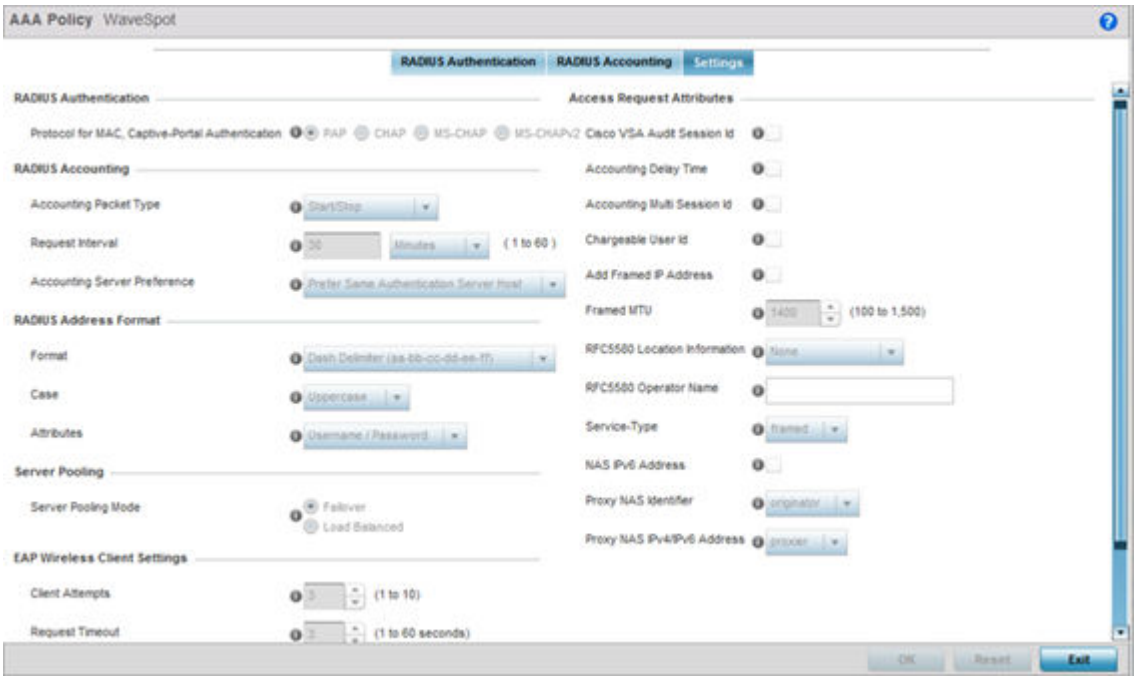
| | |
|---|---|
| Request Attempts | Displays the number of attempts a client can retransmit a missed frame to the RADIUS accounting server before it times out of the authentication session. The available range is 1 - 10 attempts. The default is 3 attempts. |
| Request Timeout | Specify the time for the access point's re-transmission of request packets. The default is 5 seconds. If this time is exceeded, the authentication session is terminated. |
| Retry Timeout Factor | Specify the interval, in seconds, between two successive re-transmission attempts of request packets. Specify a value from 50 - 200 seconds. The default is 100 seconds. |
| DSCP | Displays the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is from 0 - 63 with a default value of 34. |

13 Set the following Network Access Identifier Routing values for the accounting server:

| | |
|---|---|
| NAI Routing Enable | Check to enable NAI routing. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users in a given or without a to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS accounting servers can proxy requests to remote servers for each. |
| Realm | Enter the realm name. The name cannot exceed 64 characters. When the access point's RADIUS server receives a request for a user name, the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server. |
| Realm Type | Specify whether the Prefix or Suffix of the username is matched to the realm. |
| Strip Realm | Check strip to remove information from the packet when NAI routing is enabled. |

14 Select **Ok** to save the changes made to this window. Click **Exit** to close this window.

15 Select the **Settings** tab.




16 Set the following **RADIUS server** configuration parameters:

| | |
|---|---|
| Protocol for MAC, Captive-Portal Authentication | Set the authentication protocol when the server is used for any non-EAP authentication. Options include PAP *(Password Authentication Protocol)*, CHAP *(Challenge Handshake Authentication Protocol)*, MSPAP and MSCHAPV2. The default setting is PAP. |
| Accounting Packet Type | Set the type of RADIUS Accounting Request packets generated. Options include **`Stop Only`**, **`Start/Stop`** and **`Start/Interim/Stop`**. The default setting is Start/Stop. |
| Request Interval | Set the periodicity of the interim accounting requests to **`1 hour`**, **`1 - 60 minutes`** or **`60 - 3600`** seconds. The default is 30 minutes. |
| Accounting Server Preference | Select the server preference for RADIUS accounting. The options include:<br>• **`Prefer Same Authentication Server Host`** — Uses the authentication server host name as the host used for RADIUS accounting. This is the default setting.<br>• **`Prefer Same Authentication Server Index`** — Uses the same index as the authentication server for RADIUS accounting.<br>• **`Select Accounting Server Independently`** — Allows users to specify a RADIUS accounting server separate from the RADIUS authentication server. |
| Format | Select the format of the MAC address used in the RADIUS accounting packets. |
| Case | Lists whether the MAC address is sent using uppercase or lowercase letters. The default setting is uppercase. |
| Attributes | Lists whether the format specified applies only to the user name/password in mac-auth or for all attributes that include a MAC address, such as callingstation-id or called-station-id. |

| | |
|---|---|
| Server Pooling Mode | Controls how requests are transmitted across RADIUS servers. The options are: **`Failover`** and **`Load Balanced`**. Failover implies traversing the list of servers if any server is unresponsive. Load Balanced uses all servers in a round-robin fashion. The default setting is Failover. |
| Client Attempts | Defines the number of times (1 - 10) an EAP request is transmitted to a client before giving up. The default setting is 3. |
| Request Timeout | Set the amount of time after which an EAP request to a client is retried. The default setting is 3 seconds. |
| ID Request Timeout | Define the amount of time (1 - 60 seconds) after which an EAP ID Request to a client is retried. The default setting is 30 seconds |
| Retransmission Scale Factor | Set the scaling of the retransmission attempts. Timeout at each attempt is a function of the request timeout factor and client attempts number. 100 (default setting) implies a constant timeout at each retry; smaller values indicate more aggressive (shorter) timeouts, larger numbers set more conservative (longer) timeouts on each successive attempt. |
| Cisco VSA Audit Session Id | Set a VSA *(vendor specific attribute)* to allow CISCO's ISE *(Identity Services Engine)* to validate a requesting client's network compliance, such as the validity of virus definition files (antivirus software or definition files for an anti-spyware software application). This setting is disabled by default. |
| Accounting Delay Time | Select this option to enable the support of an accounting delay time attribute within accounting requests. This setting is disabled |
| Accounting Multi Session Id | Select this option to enable the support of an accounting multi session ID attribute. This setting is disabled by default. |
| Chargeable User Id | Select this option to enable the support of chargeable user identity. This setting is disabled by default. |
| Add Framed IP Address | Select this option to add an IP address attribute to access requests. This setting is disabled by default. |
| Framed MTU | Set the framed MTU attribute (from 100 - 1500) used in access requests. The default setting is 1400. |
| RFC5580 Location Information | Select a support option for the RFC5580 location attribute. Options include **`None`**, **`include-always`** and **`server-requested`**. The default setting is None. |
| RFC5580 Operator Name | Provide a 63 character maximum RFC5580 operator name. |
| Service-Type | Set the service type attribute value. Options include framed (default setting) and login. |
| NAS IPv6 Address | Select this option to provide support for NAS IPv6 formatted addresses when not proxying. This setting is disabled by default |
| Proxy NAS Identifier | Select a RADIUS attribute NAS identifier when proxying through the controller or RF Domain manager. Options include **`originator`** (default setting) or **`proxier`**. |
| Proxy NAS IPv6/IPv4 Address | Sets the RADIUS attribute NAS IP address and NAS IPv4 address behavior when proxying through the controller or RF Domain manager. Options include **`None`** and **`proxier`** (default setting). |

17 Select **OK** to save the updates to the AAA configuration. Select **Reset** to revert to the last saved configuration.

# AAA TACACS Policy

TACACS *(Terminal Access Controller Access - Control System+)* is a protocol created by CISCO Systems which provides access control to network devices (routers, network access servers and other networked computing devices) using one or more centralized servers. TACACS provides separate authentication, authorization, and accounting services running on different servers.

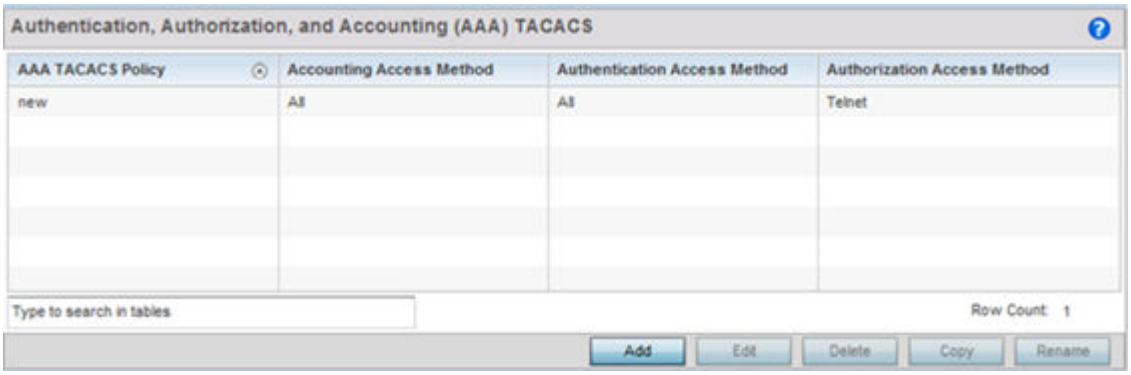
TACACS controls user access to devices and network resources while providing separate accounting, authentication, and authorization services. Some of the services provided by TACACS are:

- Authorizing each command with the TACACS server before execution
- Accounting each session's logon and log off event
- Authenticating each user with the TACACS server before enabling access to network

To define a unique AAA TACACS configuration:

1 Select **Configuration→ Network → AAA TACACS Policy**.

The Authentication, Authorization, and Accounting (AAA) TACACS screen lists existing AAA policies. Any of these policies can be selected and applied to a controller, service platform or Access Point.



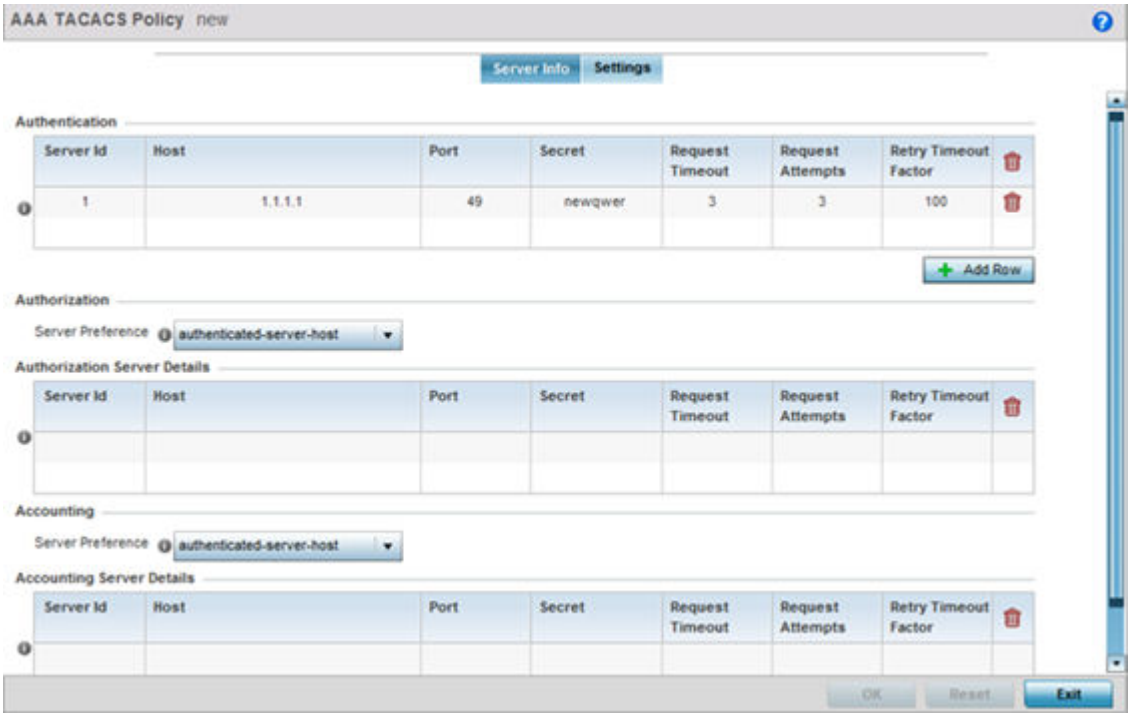

2 Refer to the following information for each existing AAA TACACS policy:

| | |
|---|---|
| AAA TACACS Policy | Displays the name assigned to the AAA TACACS policy when it was initially created. The name cannot be edited within a listed profile. |
| Accounting Access Method | Displays the connection method used to access the AAA TACACS accounting server. Options include All, SSH, Console, or Telnet. |
| Authentication Access Method | Displays the method used to access the AAA TACACS authentication server. Options include All, SSH, Console, Telnet, or Web. |
| Authorization Access Method | Displays the method used to access the AAA TACACS authorization server. Options include All, SSH, Console, or Telnet. |

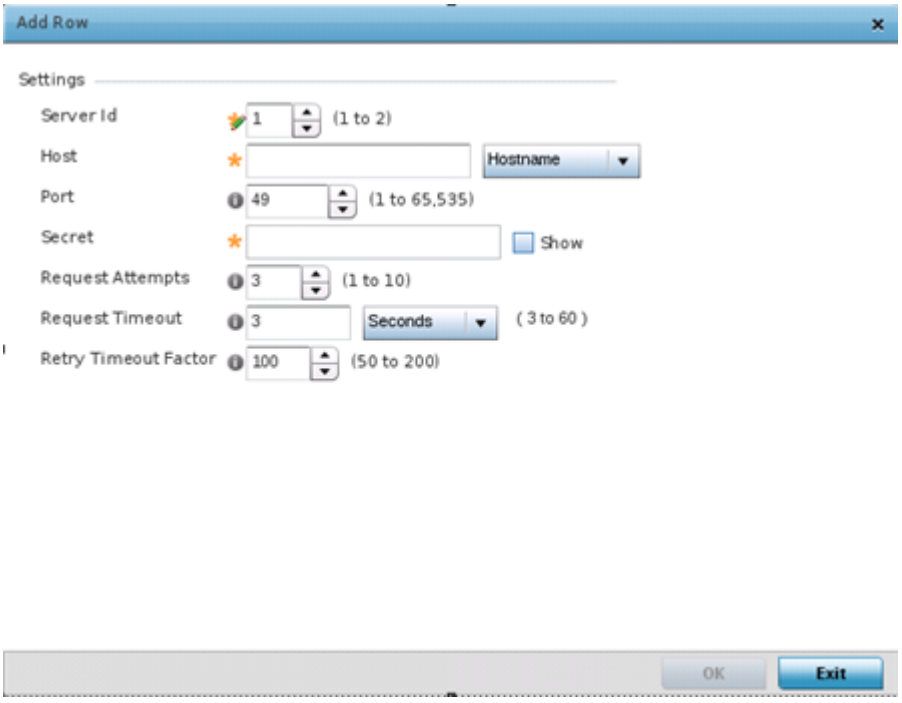
3 Select **Add** to configure a new AAA TACACS policy. Select an existing policy and use the **Edit** button to edit the policy or use the **Delete** button to delete it.

4 Provide a name for the AAA TACACS policy in the AAA TACACS Policy field. The name can be up to 32 characters long. Click **Continue**. Click **OK** to proceed.

The Server Info tab displays by default.




5 Under the **Authentication** table, select **+ Add Row**.



6 Set the following **Authentication** settings:

| | |
|---|---|
| Server Id | Set numerical server index (1-2) for the authentication server when added to the list of available TACACS authentication server resources. |
| Host | Specify the IP address or hostname of the AAA TACACS server. |
| Port | Define or edit the port on which the AAA TACACS server listens to traffic. The port range is 1 - 65,535. The default port is 49. |
| Secret | Specify (and confirm) the secret (password) used for authentication between the selected AAA TACACS server and the controller, service platform or access point. By default the secret is displayed as asterisks. To see the secret being entered, select the Show option. |
| Request Attempts | Set the number of connection request attempts to the TACACS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3. |
| Request Timeout | Specify the time for the re-transmission of request packets after an unsuccessful attempt. The default is 3 seconds. If the set time is exceeded, the authentication session is terminated. |
| Retry Timeout Factor | Set the scaling of retransmission attempts from 50 - 200 seconds. The timeout at each attempt is the function of the retry timeout factor and the attempt number. 100 (the default value) implies a constant timeout on each retry. Smaller values indicate more aggressive (shorter) timeouts. Larger numbers define more conservative (larger) timeouts on each successive attempt. The default is 100. |

7 Select **OK** to save the changes or **Exit** to close the screen.

8 Set the **Server Preference**, within the **Authorization** field, to specify which server, in the pool of servers, is selected to receice authorization requests. Options include None, authenticated-server-host, and authenticatedserver- number. If selecting None or authenticated-server-number select **+ Add Row** and set the server's ID, host, port, password and connection attempt parameters.

9 Set the following **Authorization Server** details:

| | |
|---|---|
| Server Id | Lists the numerical server index (1-2) for each authentication server when added to the list available to the controller, service platform or access point. |
| Host | Displays the IP address or hostname set for the AAA TACACS authentication server. |
| Port | Displays the port the TACACS authentication server listens to traffic. The port range is 1 - 65,535. The default port is 49. |
| Secret | Specify (and confirm) the secret (password) used for authentication between the selected AAA TACACS server and the controller, service platform or access point. By default the secret is displayed as asterisks. To see the secret being entered, select the Show option. |
| Request Attempts | Displays the number of connection attempts before the controller, service platform or access point times out of the authentication session. The available range is from 1 - 10. The default is 3. |

| | |
|---|---|
| Request Timeout | Specify the time for the re-transmission of request packets after an unsuccessful attempt. The default is 3 seconds. If the set time is exceeded, the authentication session is terminated. |
| Retry Timeout Factor | Set the scaling of retransmission attempts from 50 - 200 seconds. The timeout at each attempt is the function of the retry timeout factor and the attempt number. 100 (the default value) implies a constant timeout on each retry. Smaller values indicate more aggressive (shorter) timeouts. Larger numbers define more conservative (larger) timeouts on each successive attempt. The default is 100. |

10 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

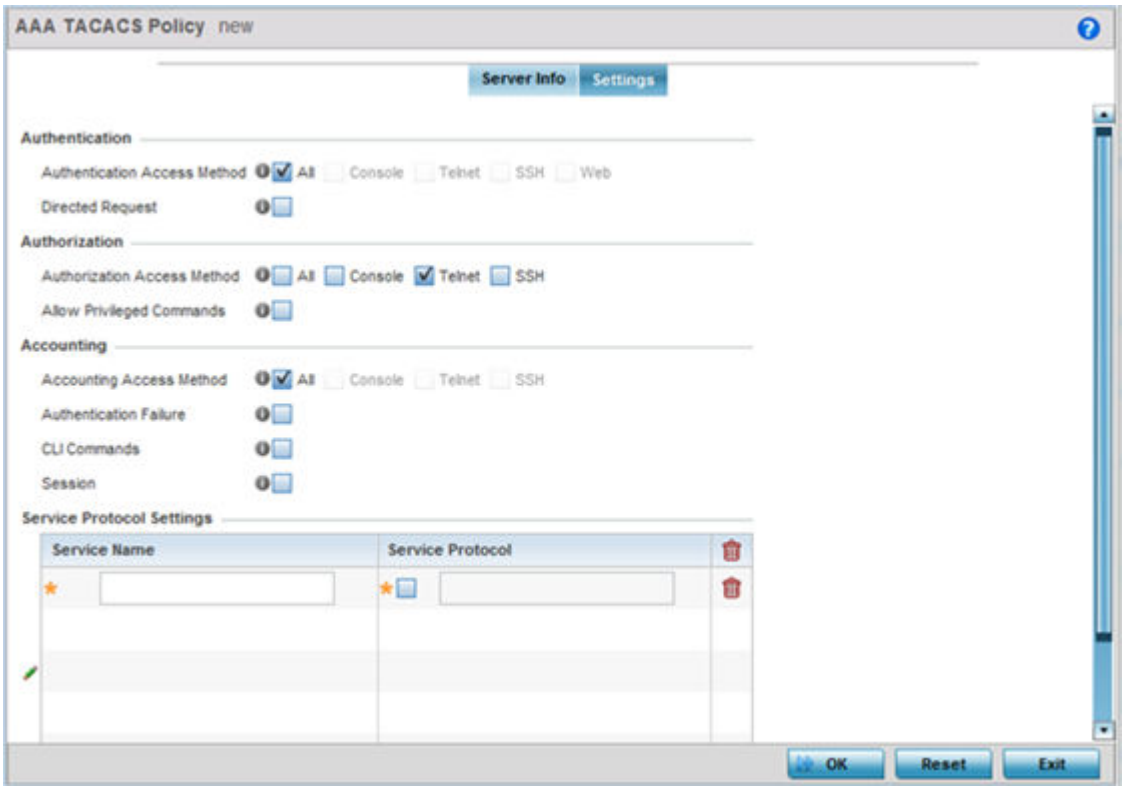
11 Set the **Server Preference**, within the Accounting field, to select the accounting server, from the pool of servers, to receive accounting requests. Options inlcude None, authenticated-server-host, authenticated-server-number, authorized-server-host and authorized-server-number. The default is authenticated-server-host. If selecting None, authenticated-server-number or authorized-server-number select **+ Add Row** and set the server's ID, host, port, password and connection attempt parameters.

12 Set the following Accounting Server details:

| | |
|---|---|
| Server Id | Lists the numerical server index (1-2) for each authentication server when added to the list available to the controller, service platform or Access Point. |
| Host | Displays the IP address or hostname set for the AAA TACACS authentication server. |
| Port | Displays the port the TACACS authentication server listens to traffic. The port range is 1 - 65,535. The default port |
| Secret | Specify (and confirm) the secret (password) used for authentication between the selected AAA TACACS server and the controller, service platform or Access Point. By default the secret is displayed as asterisks. To show the secret in plain text, select |
| Request Attempts | Displays the number of connection attempts before the controller, service platform or Access Point times out of the authentication session. The available range is from 1 - 10. The |
| Request Timeout | Specify the time for the re-transmission of request packets after an unsuccessful attempt. The default is 3 seconds. If the set time is exceeded, the authentication session is terminated |
| Retry Timeout Factor | Set the scaling of retransmission attempts from 50 - 200 seconds. The timeout at each attempt is the function of the retry timeout factor and the attempt number. 100 (the default value) implies a constant timeout on each retry. Smaller values indicate more aggressive (shorter) timeouts. Larger numbers define more conservative (larger) timeouts on each successive attempt. The default is 100 |

13 Select **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

14 Select the **Settings** tab.




15 Set the following AAA TACACS **Authentication** server configuration parameters:

| | |
|---|---|
| Authentication Access Method | Specify the connection method(s) for authentication requests.<br>• All – Authentication is performed for all types of access without prioritization.<br>• Console – Authentication is performed only for console access.<br>• Telnet – Authentication is performed only for access through Telnet.<br>• SSH – Authentication is performed only for access through SSH.<br>• Web – Authentication is performed only for access through the Web interface. |
| Directed Request | Select to enable the AAA TACACS authentication server to be used with the '@<server name>' nomenclature. The specified server must be present in the list of defined Authentication servers. |

16 Set the following AAA TACACS **Authorization** server configuration parameters:

| | |
|---|---|
| Authorization Access Method | Specify the connection method(s) for authorization requests.<br>• All – Authorization is performed for all types of access without prioritization.<br>• Console – Authorization is performed only for console access.<br>• Telnet – Authorization is performed only for access through Telnet.<br>• SSH – Authorization is performed only for access through SSH. |
| Allow Privileged Commands | Select this option to enable privileged commands executed without command authorization. Privileged commands are commands that can alter/ change the authorization server configuration. |

17 Set the following AAA TACACS Accounting server configuration parameters:

| | |
|---|---|
| Accounting Access Method | Specify the connection method(s) for accounting requests.<br>• All – Accounting is performed for all types of access without prioritization.<br>• Console – Accounting is performed only for console access.<br>• Telnet – Accounting is performed only for access through Telnet.<br>• SSH – Accounting is performed only for access through SSH. |
| Authentication Failure | Select the option to enable accounting upon authentication failures. This setting is disabled by default. |
| CLI Commands | Select this option to enable accounting for CLI commands. This setting is disabled by default. |
| Session | Select this option to enable accounting for session start and session stop events. This setting is disabled by default. |

18 Select **+ Add Row** and set the following Service Protocol Settings parameters:

| | |
|---|---|
| Service Name | Provide a 30 character maximum shell service for user authorization. |
| Service Protocol | Enter a protocol for user authentication using the service. |

Note
A maximum or 5 entries can be made in the Service Protocol Settings table.

19 Select **OK** to save the updates to the AAA TACACS policy. Select **Reset** to revert to the last saved configuration.

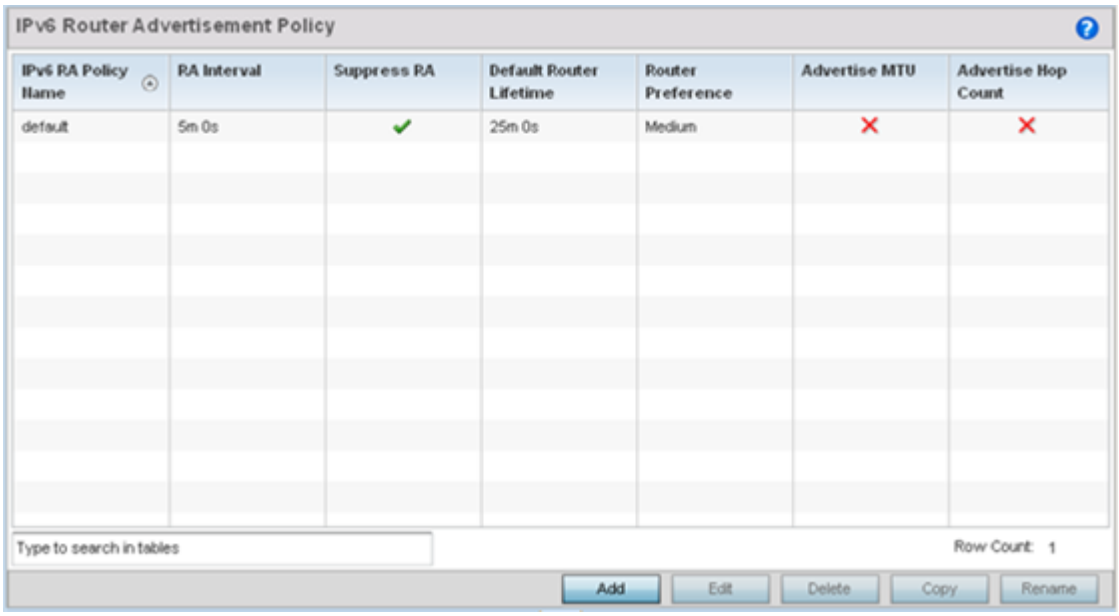
## IPv6 Router Advertisment Policy

An IPv6 router policy allows routers to advertise their presence in response to solicitation messages. After receiving a neighbor solicitation message, the destination node sends an advertisement message. which includes the link layer address of the source node. After receiving the advertisement, the destination device replies with a neighbor advertisement message on the local link. After the source receives the advertisement it can communicate with other devices.

Advertisement messages are also sent to indicate a change in link layer address for a node on the local link. With such a change, the multicast address becomes the destination address for advertisement messages.

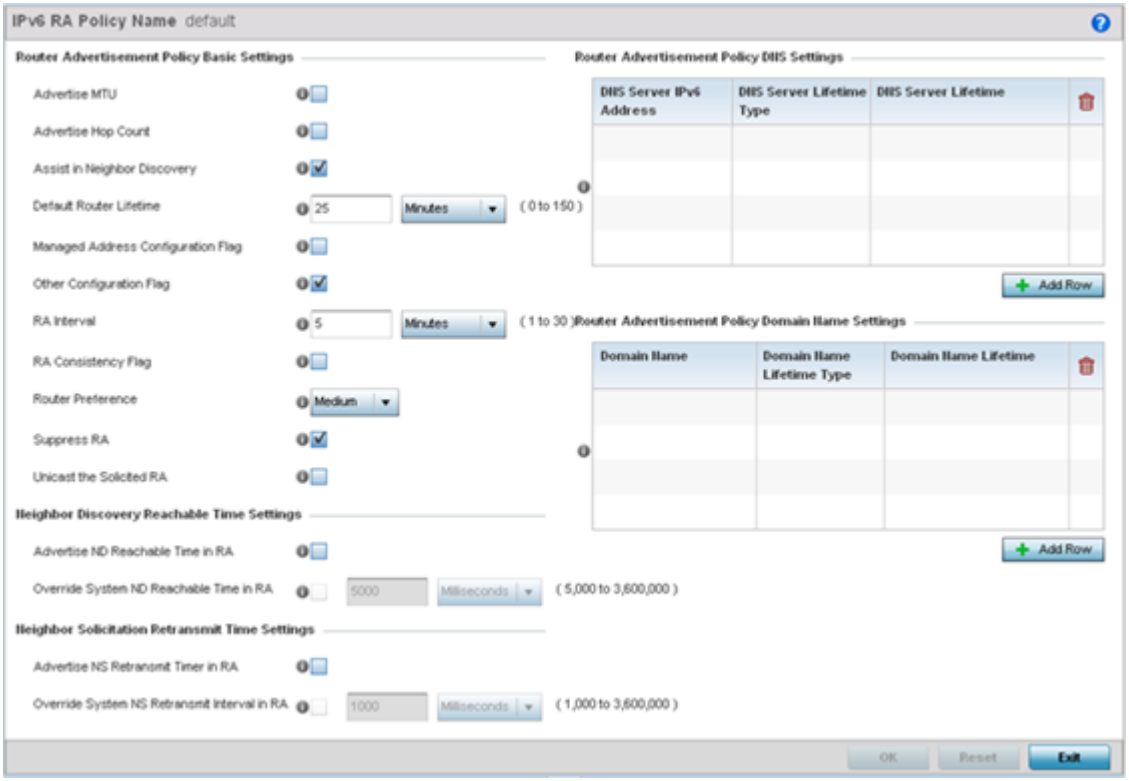
To define a IPv6 router advertisement policy:

1 Select **Configuration** > **Network** > **IPv6 Router Advertisement Policy**.




2 Select **Add** to create a new IPv6 router advertisement policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed. Provide a 32 character maximum name for the policy in the **IPv6 RA Policy Name** field. Select OK to proceed.

The IPv6 RA Policy Name screen displays.



3 Set the following **Router Advertisement Policy Basic Settings**:

| | |
|---|---|
| Advertise MTU | Select this option to include the Maximum Transmission Unit (MTU) in the router advertisements. The default setting is disabled |
| Advertise Hop Count | Select this option to include the hop count in the header of outgoing IPv6 packets. The default setting is disabled. |
| Assist in Neighbor Discovery | Select this option to send the source link layer address in a router advertisement to assist in neighbor discovery. The default setting is enabled. |
| Default Router Lifetime | Set the default router lifetime availability for IPv6 router advertisements. A lifetime of 0 indicates that the router is not a default router. The router advertisement interval range is 0 - 9000 Seconds, 0 - 150 Minutes, or 0 - 2.5 Hours. The default is 30 |
| Managed Address Configuration Flag | Select this option to send the managed address configuration flag in router advertisements. When set, the flag indicates that the addresses are available via DHCP v6. The default setting is disabled |
| Other Configuration Flag | Select this option to send the other configuration flag in router advertisements. When set, the flag indicates other configuration information (DNS related information, information on other servers within the network) is available via DHCP v6. The default |
| RA Interval | Set the interval for unsolicited IPv6 router assignments. The router advertisement interval range is 3 - 1800 seconds or 0 - 150 minutes. The default is 5 minutes. |
| RA Consistency Flag | Select this option to check if parameters advertised by other routers on the local link are in conflict with those router advertisements by this controller, service platform or Access Point. This option is disabled. |
| Router Preference | Set a High, Medium or Low preference designation on this router versus other router resource that may be available to the controller, service platform or Access Point. The default setting is medium. |
| Suppress RA | Use this setting to enable or diable the transmission of a router advertisement within the IPv6 packet. This setting is enabled by default. |
| Unicast the Solicited RA | Select this option to enable the unicast (single destination) transmission of a router advertisement within the IPv6 packet. This setting is disabled by default. |

4 Set the following Neighbor Discovery Reachable Time Settings:

| | |
|---|---|
| Advertise ND Reachable Time in RA | Select this option not specify the neighbor reachable time in the router advertisements. When unspecified, the neighbor reachable time configured for the system is advertised. The default setting is disabled. |
| Override System ND Reachable Time in RA | Set the period for sending neighbor reachable time in the router advertisements. When unspecified, the neighbor reachable time configured for the system is advertised. The interval range is from 5,000 - 3,600,000 milliseconds. The default is 5000 milliseconds. |

5 Set the following Neighbor Solicitation Retransmit Time Settings:

| | |
|---|---|
| Advertise NS Retransmit Timer in RA | Select this option to not specify the neighbor solicitation retransmit timer value in router advertisements. The default setting is disabled. |
| Override System NS Retransmit Interval in RA | Set the period for sending the neighbor solicitation retransmit timer in router advertisements. When unspecified, the setting configured for the system is advertised. The interval range is from 1000 - 3,600,000 milliseconds. The default is 1000 milliseconds. |

6 Select **+ Add Row** under the Router Advertisement Policy DNS Settings table and set the following:

| | |
|---|---|
| DNS Server IPv6 Address | Use a DNS server to resolve host names to IPv6 addresses. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. This field is mandatory |
| DNS Server Lifetime Type | Set the lifetime afforded to the DNS server resource. Options include expired, External (fixed), and infinite. The default is External (fixed). |
| DNS Server Lifetime | Set the maximum time the DNS server is available for name resolution. The interval range is from 1000 - 3,600,000 milliseconds. The default is 10 minutes. |

7 Select **+ Add Row** under the Router Advertisement Policy Domain Name Settings table and define the following settings:

| | |
|---|---|
| Domain Name | Enter a fully qualified domain name (FQDN) is an unambiguous domain name available a router advertisement resource. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. This field is mandatory. |
| Domain Name Lifetime Type | Set the DNS Server Lifetime Type. Options include expired, External (fixed), and infinite. The default is External (fixed). |
| Domain Name Lifetime | Set the maximum time the DNS domain name is available as a name resolution resource. The default is 10 minutes. |

8 Select **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

# Alias

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the Alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration → Network → Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from the **Configuration → Devices → System Profile → Network → Alias** screen. Profile aliases are available for use to a specific group of wireless controllers or access points. Alias values defined in a profile override the alias values defined within global aliases.
- *RF Domain* aliases are defined from the **Configuration → Devices → RF Domain → Alias** screen. RF Domain aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from the **Configuration → Devices → Device Overrides → Network → Alias** screen. Device aliases are utilized by a singular device only. Device alias values override global, profile or RF Domain alias configurations.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an network alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias work with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

For more information, refer to the following:


- Network Basic Alias Configuration on page 709
- Network Group Alias Configuration on page 711
- Network Group Alias Configuration on page 711

## Network Basic Alias Configuration

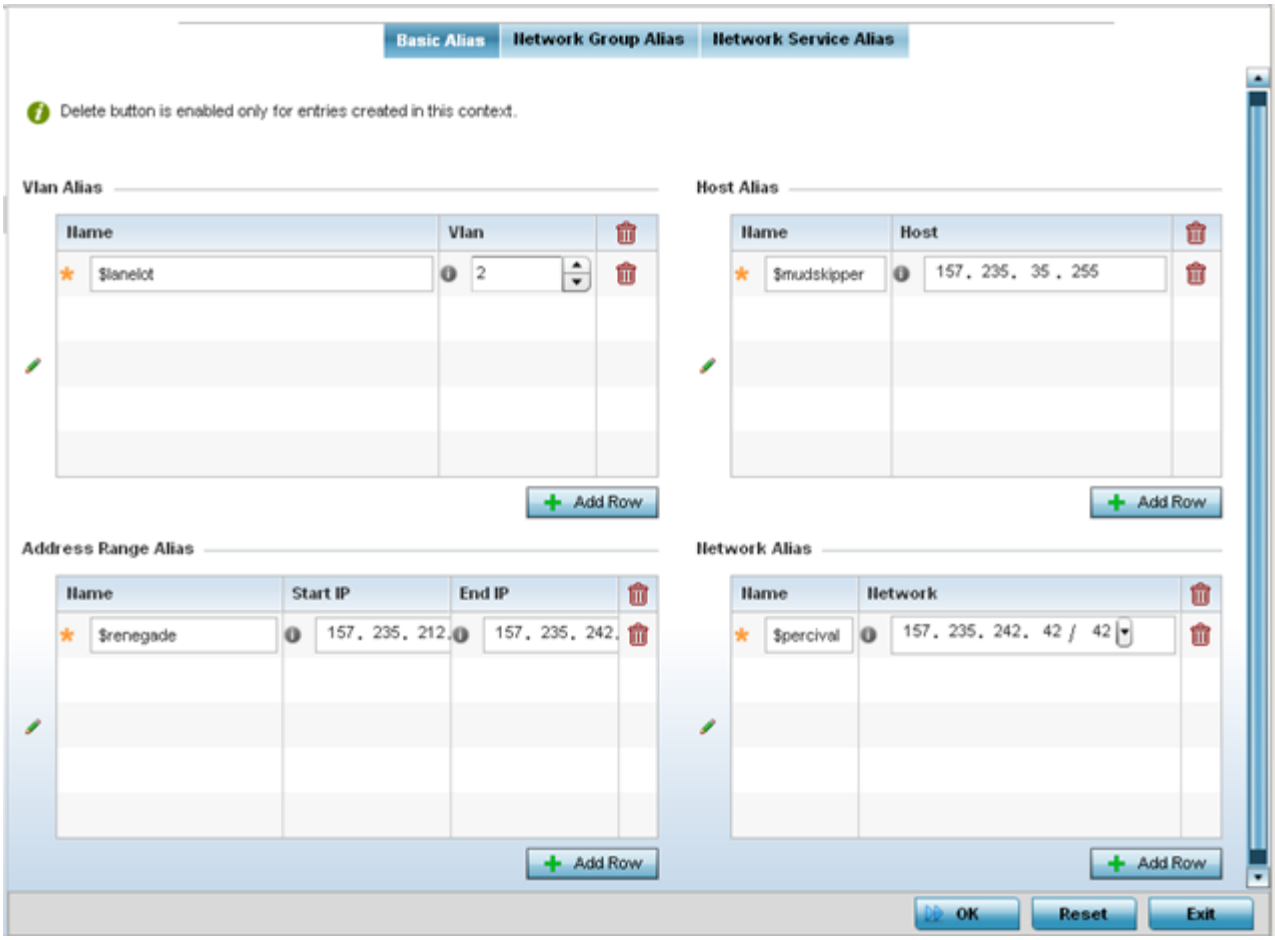
A *basic alias* is a set of configurations consisting of *VLAN, Host, Network* and *Address Range* alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

To set a network basic alias configuration:

1 Select **Configuration → Network** from the Web UI.

2 Select **Alias** from the Network menu options on the left-hand side of the UI.

The Alias screen displays with the Basic Alias tab displayed by default.




3 Select **+ Add Row** to define VLAN Alias settings:

Use the Vlan Alias field to create unique aliases for VLANs that can be utilized at different deployments. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias. At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.

| | |
|---|---|
| Name | If adding a new *VLAN Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Vlan | Use the spinner control to set a numeric VLAN ID from 1 - 4094. |

4 Select **+ Add Row** to define Address Range Alias settings:

Use the Address Range Alias field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

| | |
|---|---|
| Name | If adding a new *Address Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Start IP | Set a starting IP address used with a range of addresses utilized with the address range alias. |
| End IP | Set an ending IP address used with a range of addresses utilized with the address range alias. |

5 Select **+ Add Row** to define Host Alias settings:

Use the Host Alias field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new *Host Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Host | Set the numeric IP address set for the host. |

6 Select **+ Add Row** to define Network Alias settings:

Use the Network Alias field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

| | |
|---|---|
| Name | If adding a new *Network Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Network | Provide a network address in the form of host/mask. |

7 Select **+ Add Row** to define String Alias settings:

Use the String Alias field to create aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overriden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

| | |
|---|---|
| Name | If adding a new String Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($). |
| Value | Provide a string value to use in the alias. |

8 Select **OK** when completed to update the set of basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

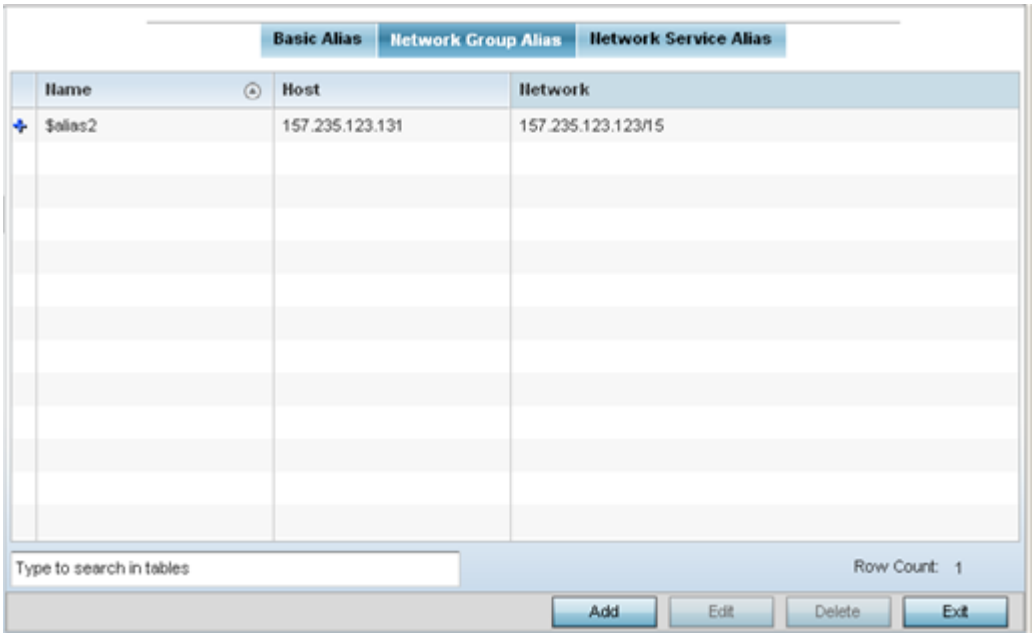
## Network Group Alias Configuration

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

To set a network group alias configuration for an IP firewall:

1 Select **Configuration** → **Network** from the Web UI.
2 Select **Alias** from the Network menu options on the left-hand side of the UI.
3 Select the **Network Group Alias** tab.




4 Review the attributes of existing network group alias configurations.

| | |
|---|---|
| Name | Displays the administrator assigned name for the network group alias. |
| Host | Displays all the host aliases configured in the listed network group alias. Displays a blank column if no host alias is defined. |
| Network | Displays all network aliases configured in the listed network group alias. Displays a blank column if no network alias is defined. |

*Adding and Editing Network Group Alias*

You can add a new network group alias configuration or edit an existing configuration.

1 Select **Add** to create a new alias, **Edit** to modify the attributes of an existing alias, or **Delete** to remove obsolete aliases.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

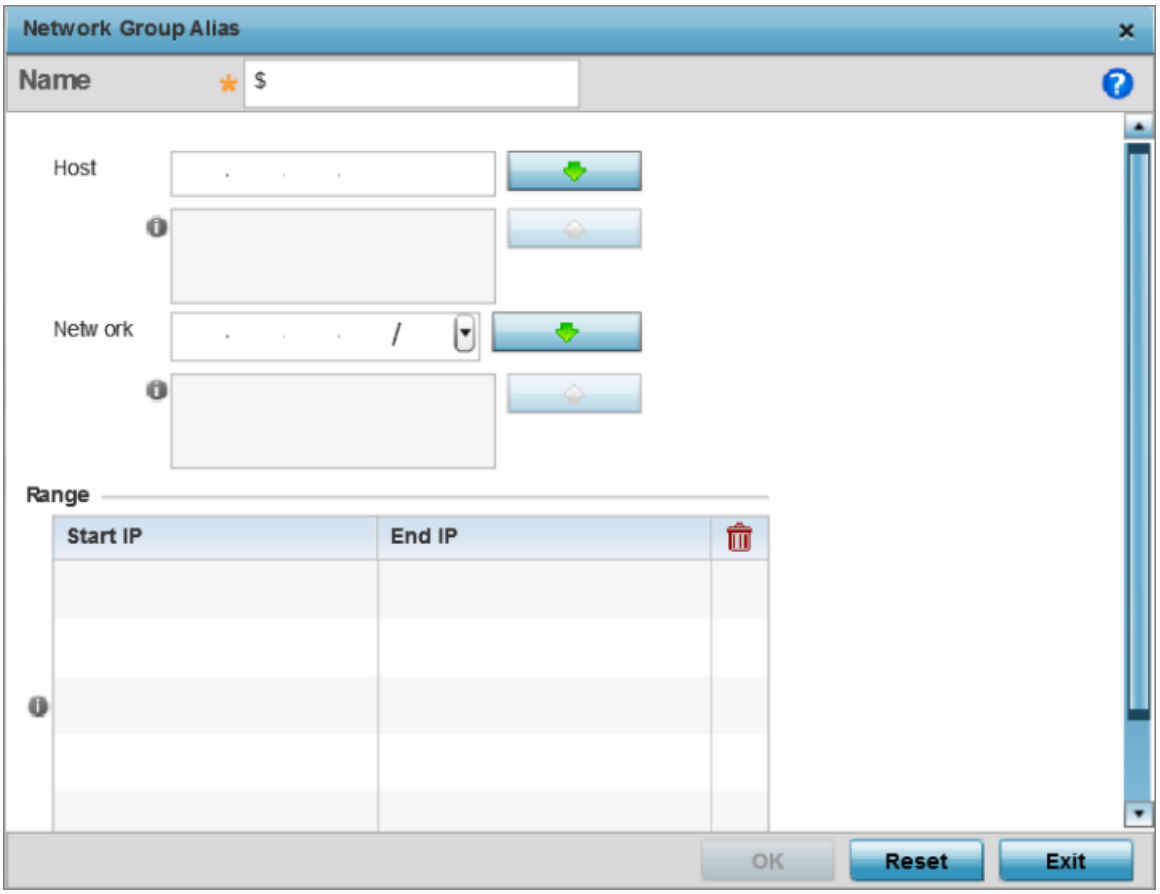



**Figure 337: Network Group Alias - Add/Edit Screen**

2 If you are adding a new network alias rule, provide a `name` up to 32 characters. The network group alias name always starts with a dollar sign ($).

3 Define the following network group alias parameters:

| | |
|---|---|
| Host | Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table. |
| Network | Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table. |

4 Select **+ Add Row**, in the Range table to specify the Start IP address and End IP address for the alias range, or double-click on an existing alias range entry to edit it.

5 Select **OK** when completed to update the network group alias settings.

Select **Reset** to revert the screen to its last saved configuration.p

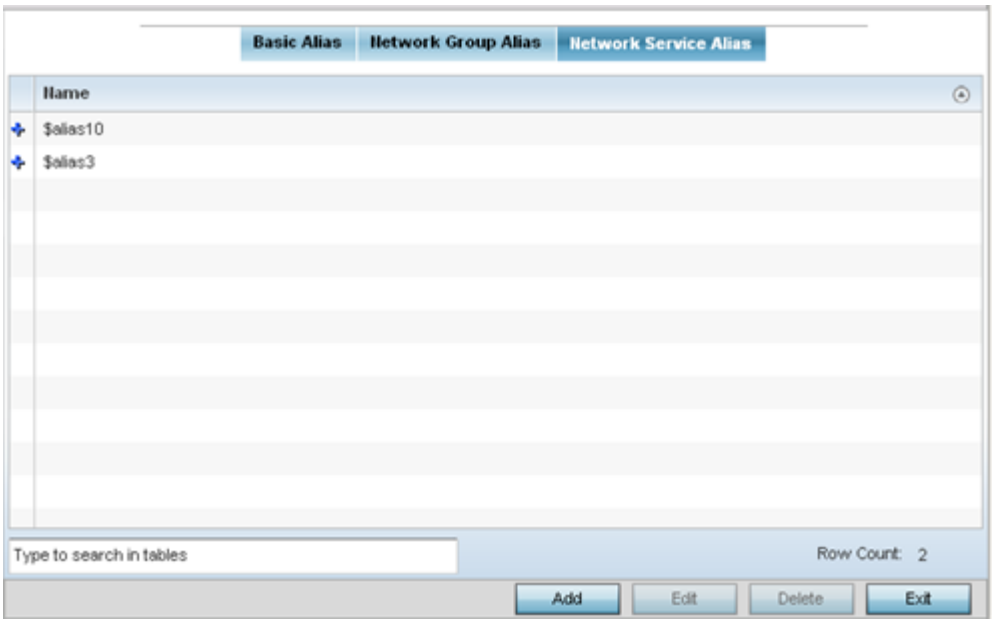
## Network Service Alias Configuration

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

To define a service alias configuration:

1 Select **Configuration** → **Network** from the Web UI.
2 Select **Alias** from the Network menu options on the left-hand side of the UI.
3 Select the **Network Service Alias** tab. The screen displays existing network service alias configurations.




### *Adding and Editing Network Service Alias*

You can add a new network service alias configuration or edit an existing configuration.

1 Select **Add** to create a new network service alias.

Select an existing network service alias and click **Edit** to modify it. Select **Delete** to remove an existing network service alias from those available in the list.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

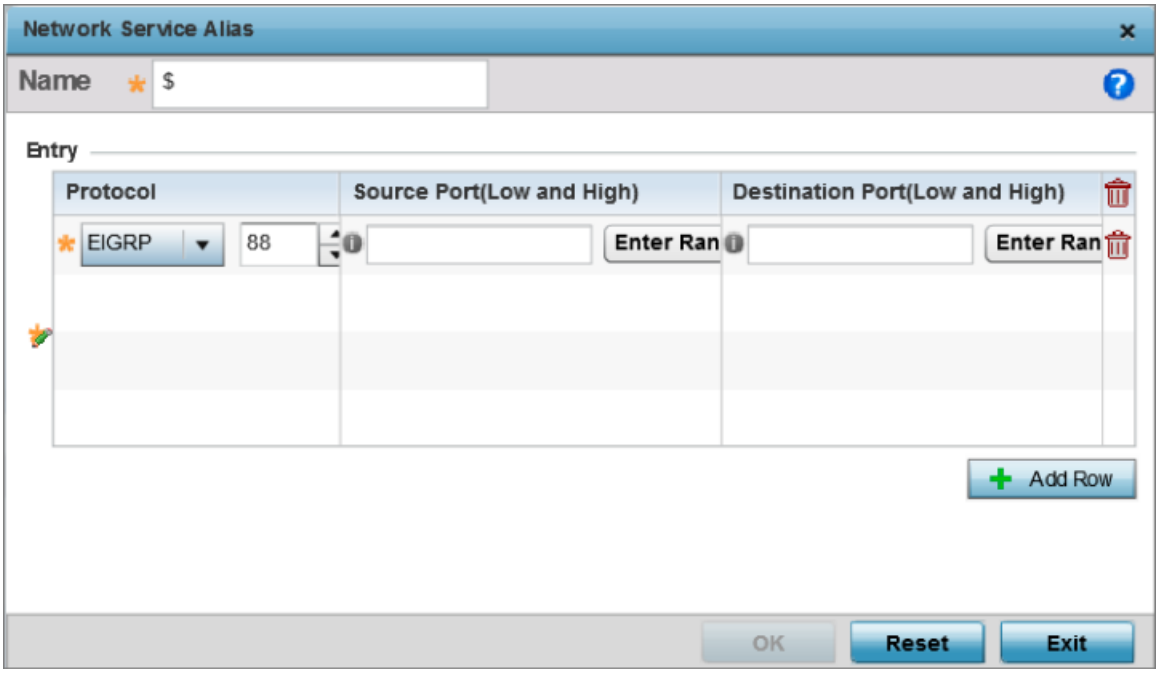



**Figure 338: Network Alias - Network Service Alias Add screen**

2 If you are adding a new Network Service Alias, give it a `Name` up to 32 characters to distinguish this alias configuration from others with similar attributes.

Note

The Network Service Alias name always starts with a dollar sign ($).

3 Select **+ Add Row**, in the Entry table and specify the following parameters:

| | |
|---|---|
| Protocol | Specify the protocol for which the alias is created. Use the drop down to select the protocol from **`eigrp`**, **`gre`**, **`icmp`**, **`igmp`**, **`ip`**, **`vrrp`**, **`igp`**, **`ospf`**, **`tcp`** and **`udp`**. Select **`other`** if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected. |
| Source Port (Low and High) | This field is relevant only if the protocol is *tcp* or *udp*.<br>Specify the source ports for this protocol entry. A range of ports can be specified. Select the **Enter Range** button next to the field to enter a lower and higher port range value. Up to eight (8) ranges can be specified. |
| Destination Port (Low and High) | This field is relevant only if the protocol is *tcp* or *udp*.<br>Specify the destination ports for this protocol entry. A range of ports can be specified. Select the **Enter Range** button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified. |

4 Select **OK** when completed to update the network service alias rules.

Select **Reset** to revert the screen back to its last saved configuration.

# Application Policy

When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. An application policy defines the rules or actions executed on recognized applications (for example, Facebook) or application-categories (for example, socialnetworking). The following are the rules/actions that can be applied in an application policy:

- Allow - Allow packets for a specific application or application category
- Deny - Deny packets for a specific application or application category
- Mark - Mark packets with DSCP/8021p value for a specific application or application category
- Rate-limit - Rate limit packets from specific application types

For each rule defined, a precedence is assigned to resolve conflicting rules for applications and categories. A deny rule is exclusive, as no other action can be combined with a deny. An allow rule is redundant with other actions, since the default action is allow. An allow rule is useful when wanting to deny packets for a category, but wanting to allow a few applications in the same category to proceed. In such a cases, add an allow rule for applications with a higher precedence then a deny rule for that category.

Mark actions mark packets for a recognized application and category with DSCP/8021p values used for QoS. Ratelimits create a rate-limiter applied to packets recognized for an application and category. Ingress and egress rates need to be specified for the rate-limiter, but both are not required. Mark and rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

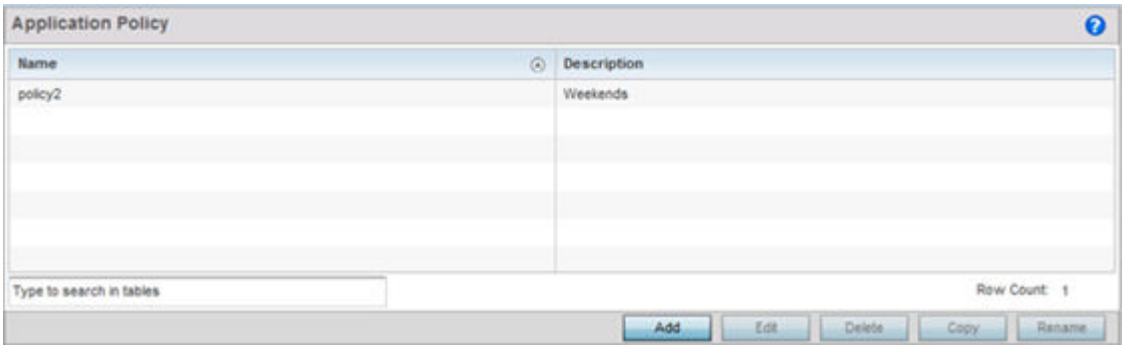
Note

The WiNG 7.1 release does not support DPI on the AP505i and AP510i model access points. This feature will be supported in future releases.

To define an application policy configuration:

1 Select **Configuration → Network → Application Policy**.

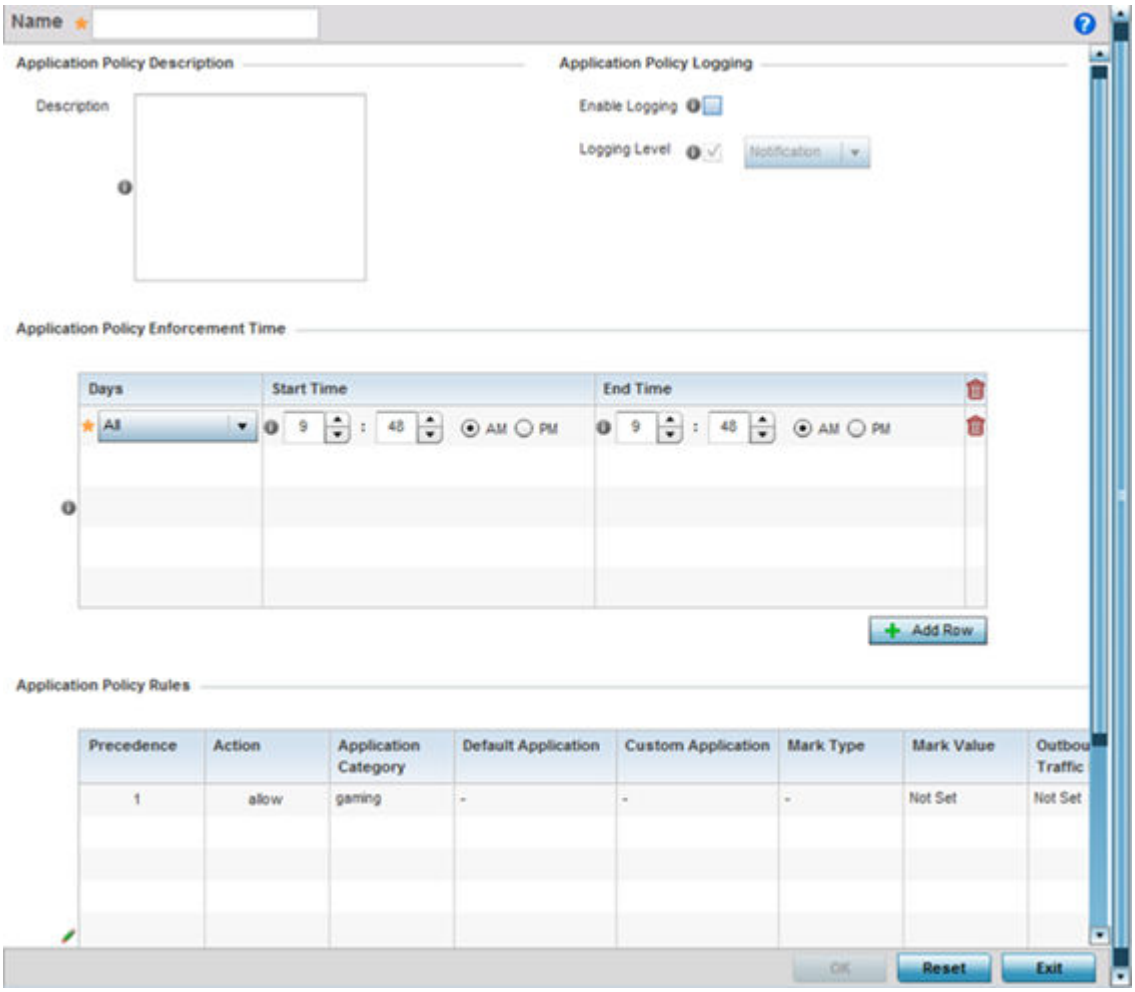
The screen lists the application policy configurations defined thus far.



2 Refer to the following to determine whether a new application policy requires creation, modification or deletion:

| | |
|---|---|
| Name | Lists the 32 character maximum name assigned to each listed application policy, designated upon creation. |
| Description | Displays the 80 character maximum description assigned to each listed application policy, as a means of further distinguishing policies with similar configurations. |

3 Select **Add** to create a new application policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed.




4 If creating a new application policy, assign it a **Name** up to 32 characters.

5 Provide this application policy an 80 character maximum **Description** to highlight its application and category filters and differentiate it from other policies with similar configurations.

6 Define the following Application Policy Logging options to enable and filter logging for application specific packet flows:

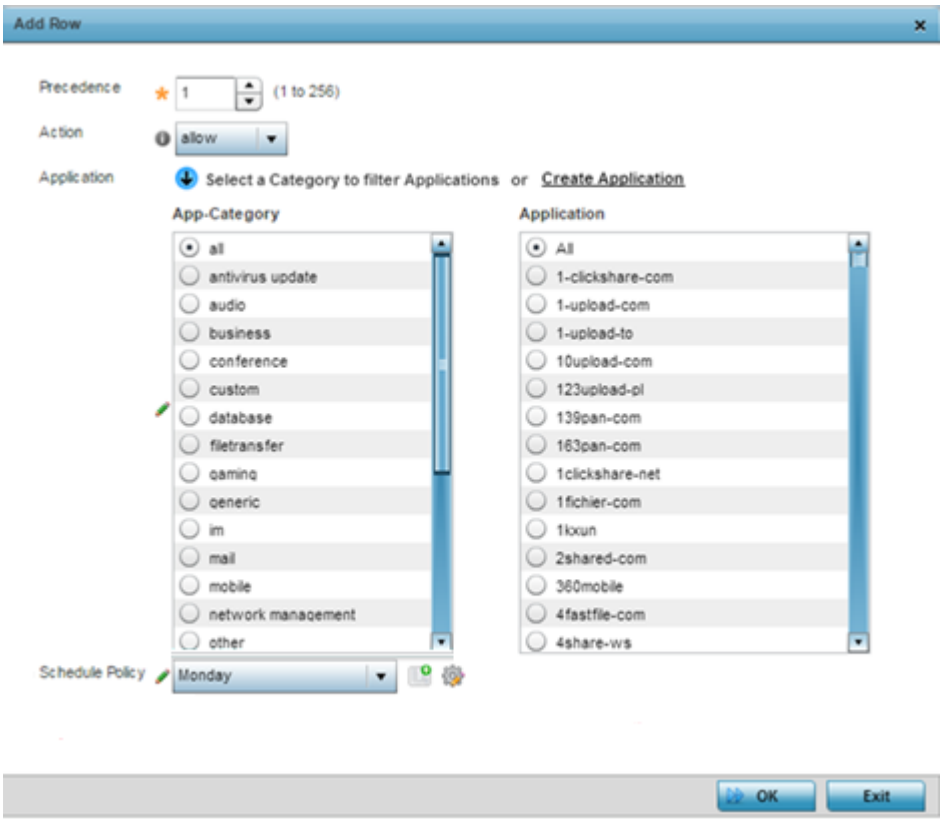
| | |
|---|---|
| Enable Logging | Enables the log functionality, where each new flow is shown with the corresponding matched application, the action taken and the policy name. When enabled, logging just shows what applications are getting recognized. |
| Logging Level | Select this option to log application events by severity. Severity levels include Emergency, Alert, Critical, Errors, Warning, Notification, Information and Debug. The default logging level is Notification. |

7 Refer to the Application Policy Enforcement Time table configure time periods for policy activation for each policy.

Select **+ Add Row** to populate the table with an enforcement time configuration to activate application policies based on the current local time. The option to configure a time activation period is applicable for a single application policy. Configure the days and time period when the application policy is enforced. If no time enforcement configuration is set, the policy is continually in effect without restriction.

8 Refer to the Application Policy Rules table assess existing policy rules, their precedence (implementation priority), their actions (allow, deny etc.), application category and schedule policy enforcement restrictions.

9 Select **+ Add Row** to launch a screen to create a new policy rule.



10 Assign the following attributes to the new application rule policy:

| | |
|---|---|
| Precedence | Set the priority (from 1 - 256) for the application policy rule. The lower the value, the higher the priority assigned to this rule's enforcement action and the category and application assigned. A precedence also helps resolve conflicting rules for applications and categories. |
| Action | Set the action executed on the selected application category and application. The default setting is Allow. |
| Application | From the App-Category table, select the category for which the application rule applies. Selecting All auto-selects All within the Application table. Select All from the Application table to list all application category statistics, or specify a particular category name to display its statistics only. |

11 Use the **Schedule Policy** drop-down menu to select an existing schedule policy to strategically enforce application filter policy rules for specific intervals. This provides stricter, time and schedule based, access or restriction to specific applications and their parent categories. If an existing policy does not meet requirements, either select the **Create** icon to configure a new policy or the **Edit** icon to modify an existing policy. For more information on configuring schedule policies, see Schedule Policy on page 723

12 Select **OK** to save the updates to the application policy.

Select **Reset** to revert to the last saved configuration.

## Application

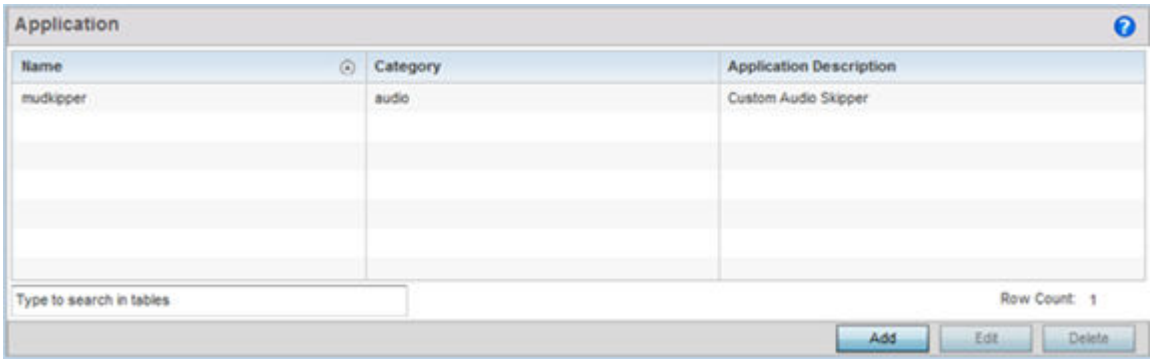
Use the Application screen to create custom application configurations.

Note
The WiNG 7.1 release does not support DPI on the AP505i and AP510i model access points. This feature will be supported in future releases.

To create a user-defined application:

1 Select **Configuration → Network → Application**.

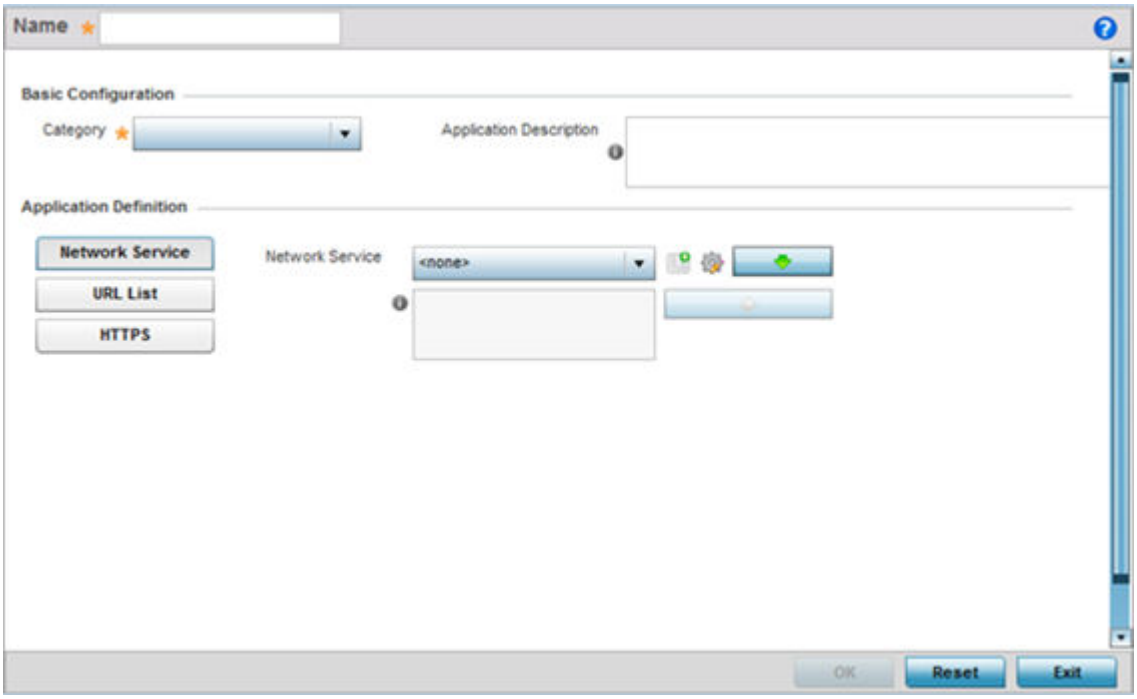
The Application screen displays. This screen lists the application configurations defined thus far.



2 Refer to the following to determine whether a application requires creation, modification or deletion:

| | |
|---|---|
| Name | Displays the name of each user-defined application created using this application interface. |
| Category | Lists the category to which each listed user-defined application belongs. |
| Application Description | Lists the 80 character maximum description administratively assigned to each listed user-defined application. |

3 Select **Add** to create a new application configuration, **Edit** to modify the attributes of a selected application or **Delete** to remove obsolete applications from the list of those available.




4 If creating a new user-defined application type, assign it a **Name** up to 32 characters. Ensure you do not create confusion by naming a user-defined application with the same name as an existing application appearing the Application Policy screen.

5 Use the **Category** list to classify the application. Select the appropriate pre-defined category or select **custom** to create a custom classification for the application.

6 Provide an 80 character maximum **Application Description** to each new user-defined application to further differentiate it from existing applications.

7 Refer to the **Application Definition** field to assign either a network service alias, predefined URL list or set of HTTPS parameters to the user-defined application.

| | |
|---|---|
| Network Service | Use the drop-down menu to select an existing network service alias for the user-defined application. If there are no existing network service alias suited to this new user-defined application, select the **Create** icon to define a new alias or the Edit icon to modify an existing one. Provide or modify a 32 character maximum name, along with a protocol type or number and source and destination port value. Up to four (4) service aliases can be supported. |
| URL List | defined application. URL lists are utilized for whitelisting and blacklisting Web application URLs from being launched and consuming bandwidth within the WiNG managed network. If no URL list suits this new user-defined application, select the **Create** icon to define a new list or the **Edit** icon to modify an existing URL list. |
| HTTPS | Select the **+ Add Row** button to populate the table with configurable rows for HTTPS parameter type, attribute type, match criteria for the HTTPS server name and 64 character maximum server name attribute used in the HTTPS server message exchange. |

8 Select **OK** to save the updates to the user-defined application configuration.

Select **Reset** to revert to the last saved configuration.

## Application Group

An application group is a heterogeneous, user-defined collection of system-provided and/or user-defined applications and application categories. It consists of multiple applications grouped together to form a collection. Use this option to review/edit existing application groups and create new application groups.

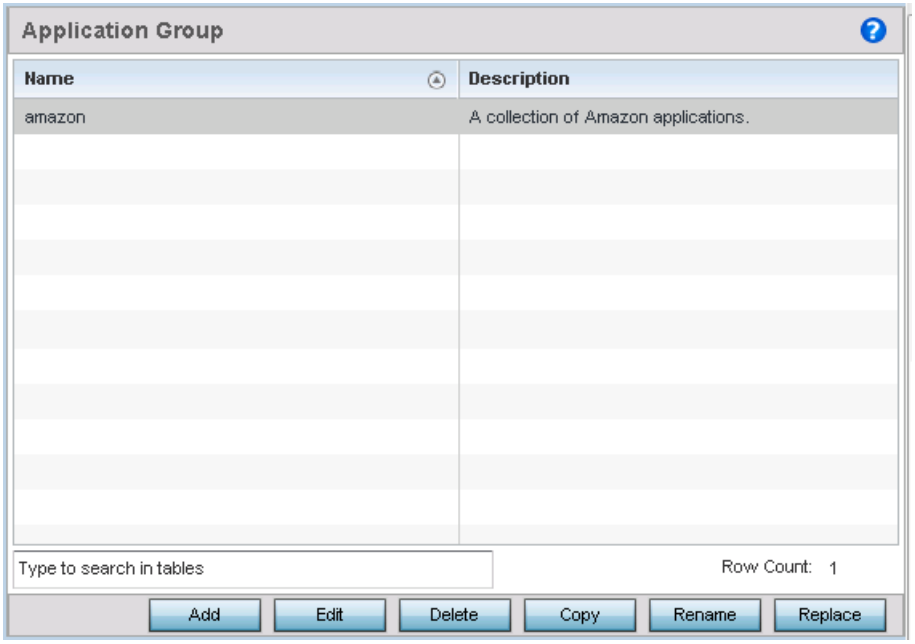
Note

The WiNG 7.1 release does not support DPI on the AP505i and AP510i model access points. This feature will be supported in future releases. This feature will be supported in future releases.

To review an application group:

1 Select **Configuration → Network → Application Group**.

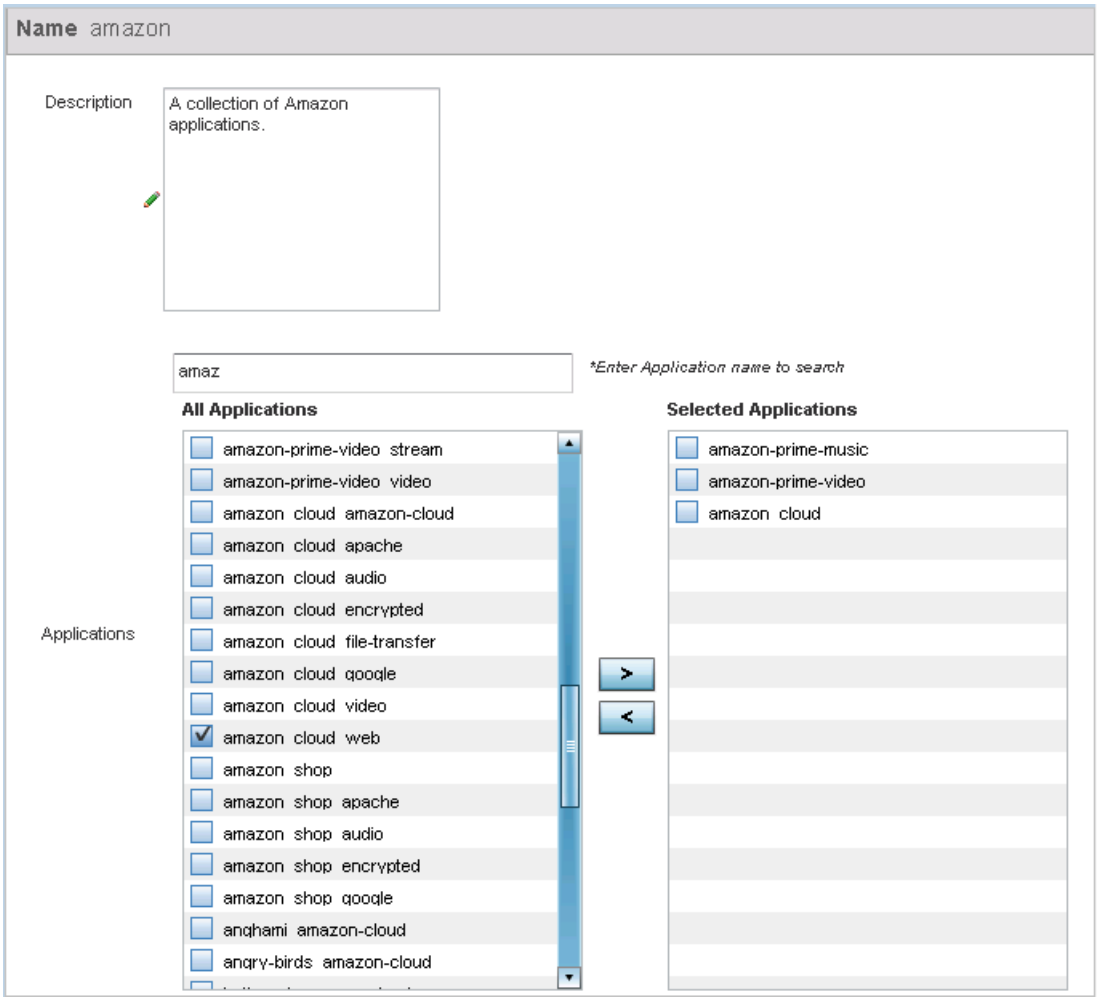
The screen lists the existing application group configurations. You can edit and existing application group or create a new application group.




2 Refer to the following to determine whether an application group requires creation, modification or deletion:

| | |
|---|---|
| Name | Displays the name of each user-defined application group |
| Description | Displays the description assigned to each listed user-defined application group. |

3 Select **Add** to create a new application group configuration, **Edit** to modify the attributes of a selected application group or **Delete** to remove obsolete application groups from the list of those available.




4 If creating a new application group, assign a **Name** not exceeding 32 characters in length. Ensure that the name uniquely differentiates it from existing application groups.

5 Provide an 80 character maximum Description to further differentiate the new group from existing application groups

6 Refer to the All Applications field. This field lists available applications - system-provided and user-defined. The WiNG software has 299 built-in applications, in addition to the user-defined ones. To facilitate your search, enter a string value in the ***Enter Application name to search** field. Based on the search string provided, the **All Applications** list is updated to display applications containing the specified string.

7 Select the applications to be included in the application group and move to the **Selected Applications** list.

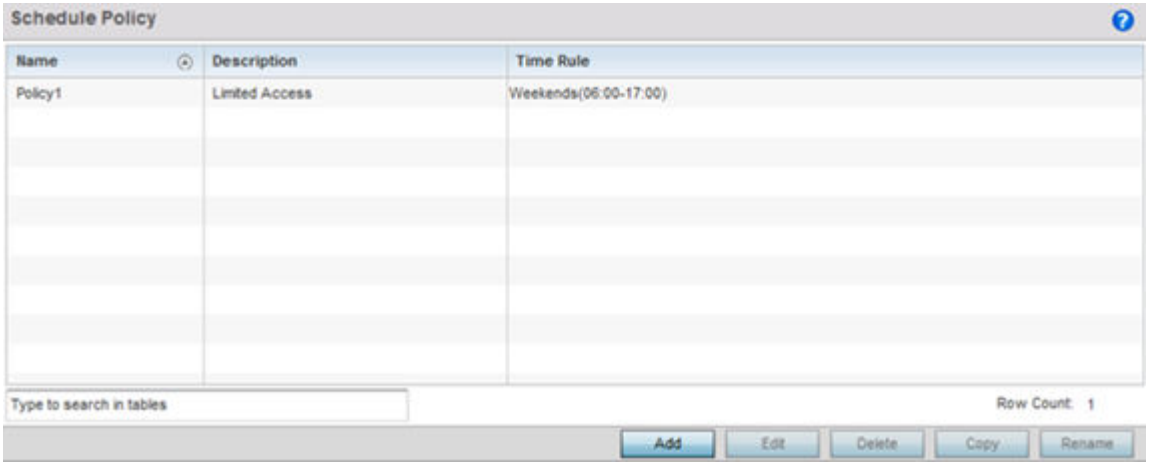
8 Select **OK** to save the updates to the application group configuration.

Select **Reset** to revert to the last saved configuration.

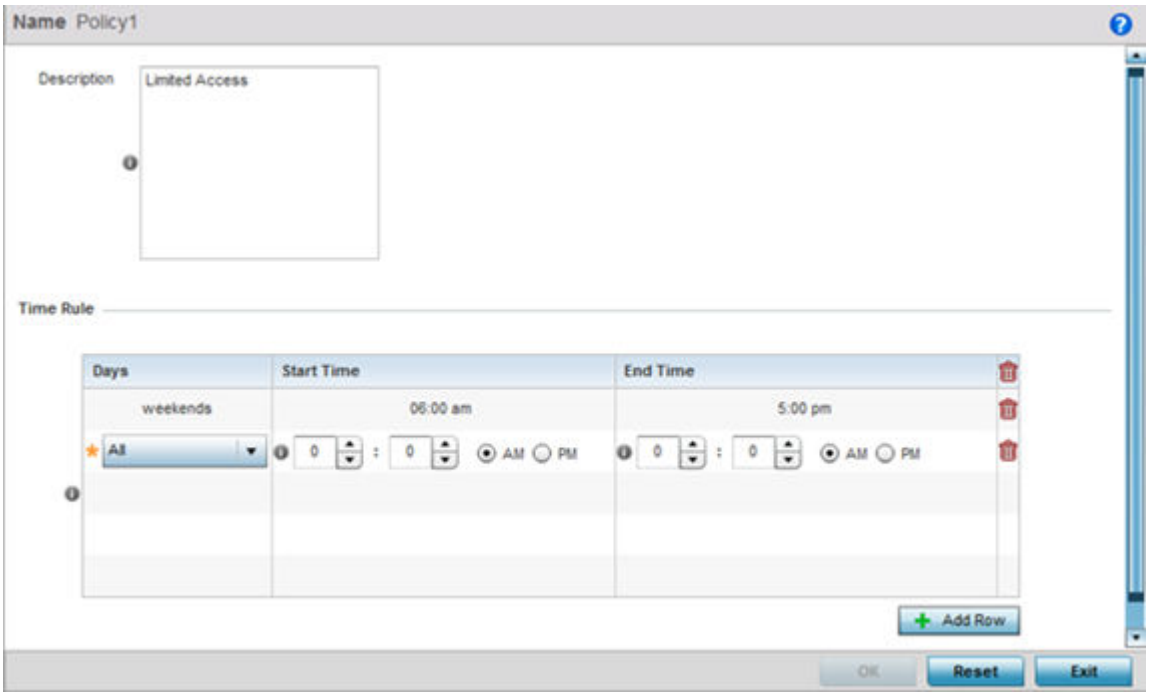
## Schedule Policy

Define schedule policies to strategically enforce application filter policy rules for specific intervals. This provides stricter, time and schedule based, access or restriction to specific applications and their parent categories. To review existing schedule policies and assess whether new ones require creation or modification:

1 Select **Configuration → Network → Schedule Policy**.




2 Select **Add** to create a new schedule policy time rule, or select an existing policy then **Edit** to modify the duration of an existing time rule. Schedule policies can be **Deleted** as they become obsolete. **Copy** or **Rename** a schedule policy as needed.




3 If creating a new schedule policy time rule configuration, enter a 32 character maximum **Name** relevant to its specific permissions objective.

4 Provide this schedule policy an 80 character maximum Description to differentiate it from other policies with similar time rule configurations.

5 Define the following **Time Rule** settings:

| | |
|---|---|
| Days | Use the drop-down menu to select a day of the week to apply this schedule policy time rule. Selecting All applies the schedule policy every day (no enforcement rule restrictions). Selecting weekends applies the policy on Saturdays and Sundays only. Selecting weekdays applies the policy on Monday, Tuesday, Wednesday, Thursday and Friday only. Selecting individual days of the week applies the policy only on just selected day. |
| Start Time | Set the start when the schedule policy time rule applies. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose AM or PM. |
| End Time | Set the ending time when the time rule is no longer enforced. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose AM or PM. |

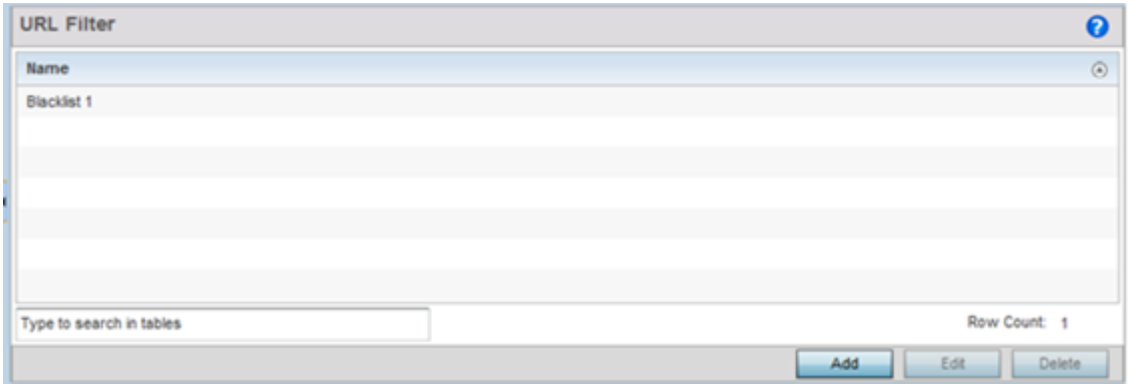
6 Select **OK** to save the updates to the schedule policy time rule configuration. Select **Reset** to revert to the last saved configuration.

## URL Filtering

A URL filter is Web content filter. A URL filter is comprised of several filter rules. To construct a filter rule, either whitelist or blacklist a filter level, category type, category or a custom category. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

To review existing URL filter rules and assess whether new ones require creation or modification:

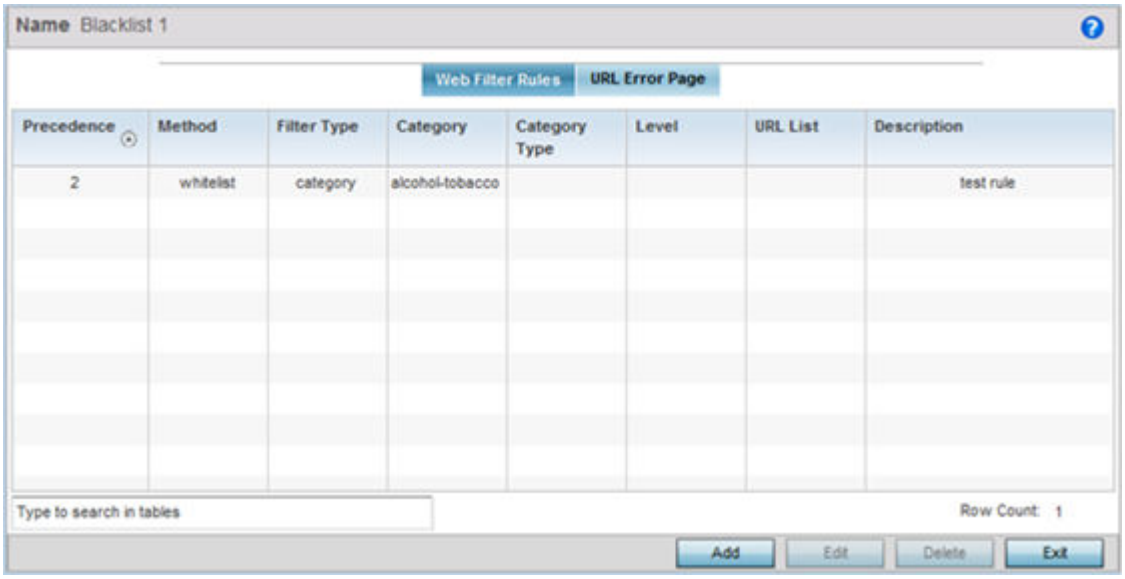
1 Select **Configuration** → **Network** → **URL Filter**.



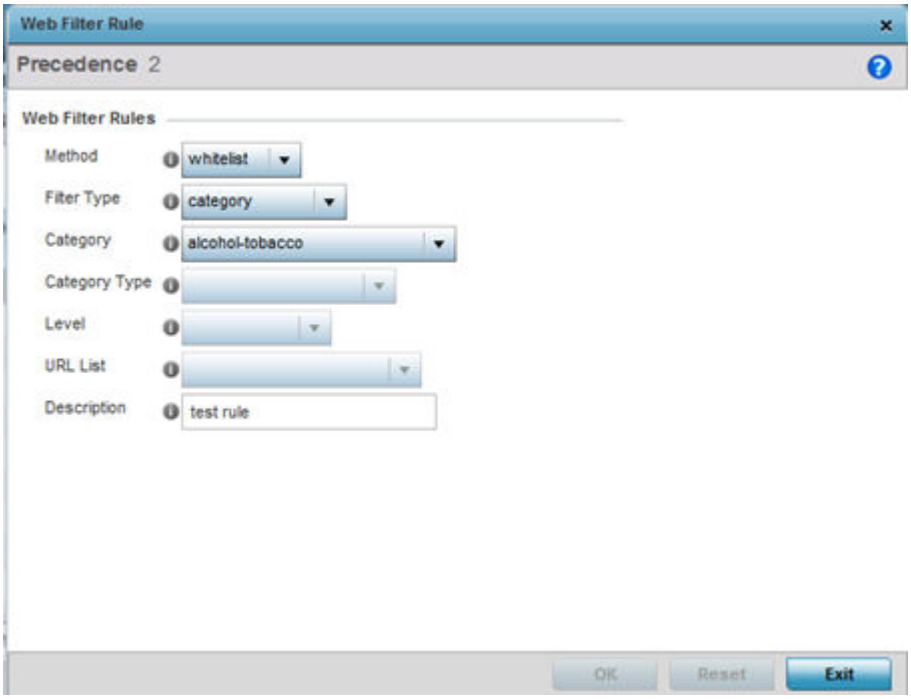

2 Select **Add** to create a new URL Filter, **Edit** to modify the attributes of a selected URL Filter or **Delete** to remove obsolete filters from the list of those available.

3 If creating a new URL Filter, assign it a Name up to 32 characters to distinguish this URL Filter from others with similar attributes. Select **Continue** to proceed to the URL Filter screen where Web filter rules and URL error page messages can be added, modified or removed. Select **Exit** to exit without creating a new URL Filter.

The URL Filter screen displays, with the Web Filter Rules tab selected by default.




4 Select **Add** to create a new Web filter rule configuration, or select an exiting configuration then Edit to modify the attributes of an existing Web filter rule.

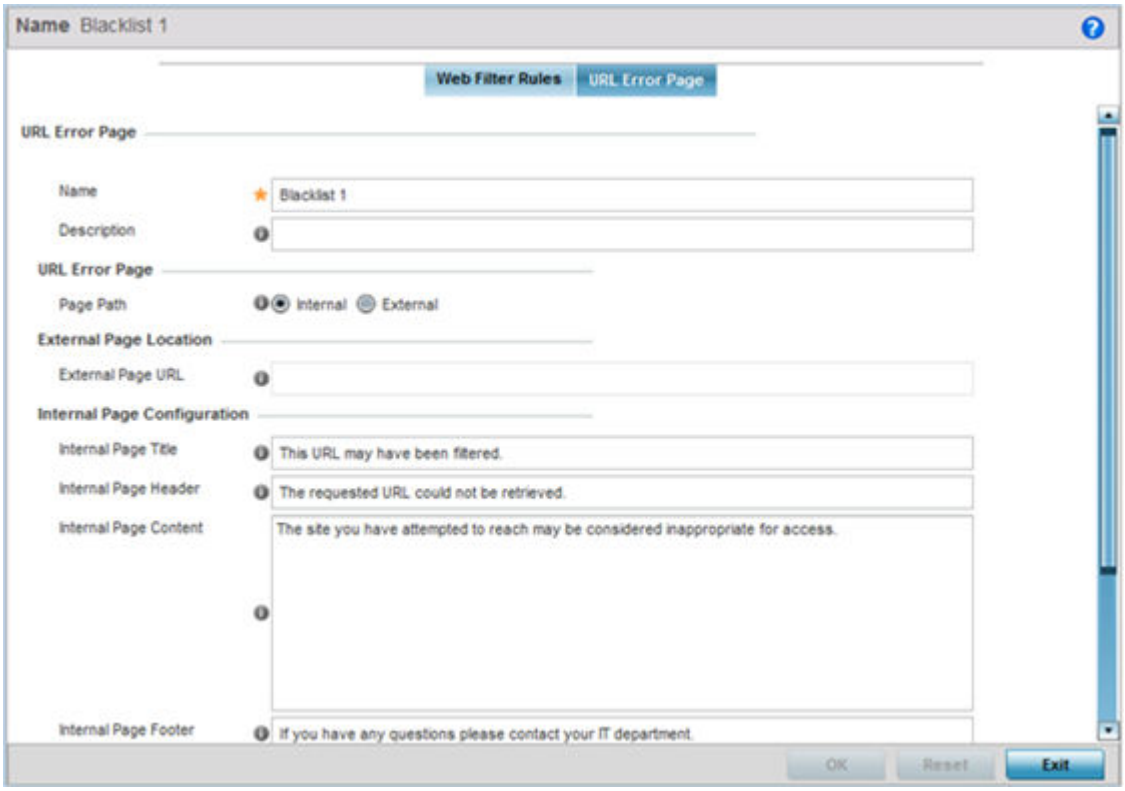


5 Define the following Web Filter Rule settings:

| | |
|---|---|
| Precedence | Set a precedence (priority) from 1 - 500 for the filter rule's utilization versus other Web filter rules. 1 is the highest priority and 500 the lowest. |
| Method | Select either whitelist or Blacklist to specify whether the rule is for inclusion or exclusion. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist. |
| Filter Type | If the Filter Type is set to category, use the drop down menu to select from a list of predefined categories to align with the whitelist or blacklist Method designation and the precedence assigned. |
| Category | A category is a pre-defined URL list available in the WiNG software. If category is selected as the Filter Type, the Category drop-down menu becomes enabled for the selection of an existing URL type or whitelist or blacklist. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the URL List and added to the database. |
| Category Type | When category_type is selected as the Filter Type, select an existing category type (adult-content, security-risk etc.) and either blacklist or whitelist the URLs in that category type. There are 12 category types available. |
| Level | Basic, Low, Medium, medium-high and High filter levels are available. Each level is pre-configured to use a set of category types. The user cannot change the categories in the category types used for these pre-configured filter-level settings, and add/modify/remove the category types mapped to the filter-level setting. |
| URL List | URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories. |
| Description | Enter a 80 character maximum description for this Web filter rule to help differentiate it from others with similar category include or exclude rule configurations. |

6 Select **OK** to save the changes to the Web Filter Rule. Select **Exit** to close the screen without saving the updates.

7 Select the URL Error Page tab to define the configuration and layout of a URL error page launched when a Web filter rule is invoked and an error page needs to be displayed to a user instead of their expected Web page.




8 Set the following URL Error Page display properties:

| | |
|---|---|
| Name | Provide a 32 character maximum name for the title of the blocking page. The name should help convey that this page is launched to prevent the client's requested page from displaying. |
| Description | Provide a 80 character maximum description of the page to help differentiate it from other pages with similar page restriction properties. |
| Page Path | Set the path to the page sent back to the client browser explaining the reason for blocking the client's requested URL. It can be generated internally at the time the page is sent, or be a URL to an External Web server if the administrator chooses to utilize a customized page. The default setting is Internal, requiring the administrator to define the page configuration within the fields in the Internal Page Configuration portion of the screen. |
| Extrernal Page URL | If External is selected as the Page Path, provide a 511 character maximum External Page URL used as the Web link designation of the externally hosted blocking page. |
| Internal Page Title | Either enter a 255 character maximum title for the URL blocking page or use the existing default text (This URL may have been filtered). |
| Internal Page Header | Either enter a 255 character maximum header for the top of the URL blocking page or use the existing default text (The requested URL could not be retrieved). |
| Internal Page Content | Enter a 255 character maximum set of text used as the main body (middle portion) of the blocking page. Optionally use the default message (The site you have attempted to reach may be considered inappropriate for access). |

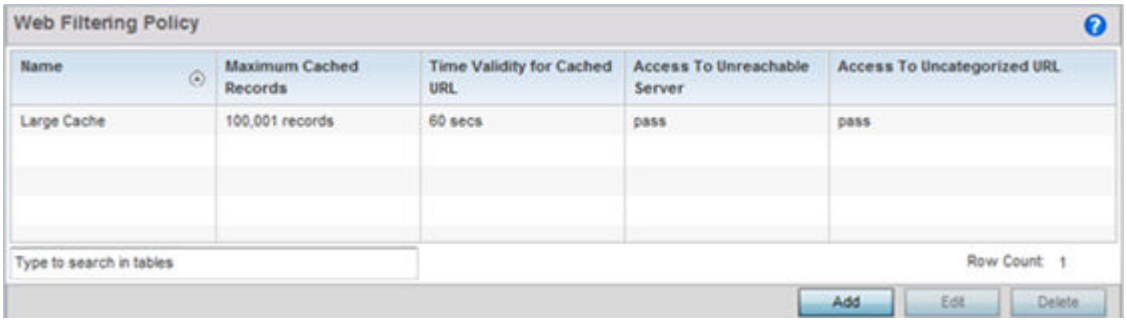
| | |
|---|---|
| Internal Page Footer | Either enter a 255 character maximum footer for the bottom of the URL blocking page or use the existing default text (If you have any questions contact your IT department). |
| Internal Page Org Name | Enter a 255 character maximum organizational name responsible for the URL blocking page. The default organizational name (Your Organizational Name) is not very practical, and is just a guideline for customization. |
| Internal Page Org Structure | Enter a 255 character maximum organizational signature responsible for the URL blocking page. The default organizational signature (Your Organizational Name, All Rights Reserved) is not very practical, and is just a guideline for customization. |
| Internal Page Logo 1 | Provide the location and filename of a small graphic image displayed in the blocking page. |
| Internal Page Logo 2 | Provide the location and filename of a main graphic image displayed in the blocking page. |

9 Select **OK** to save the updates to the URL filter configuration. Select **Reset** to revert to the last saved configuration.

## Web Filtering

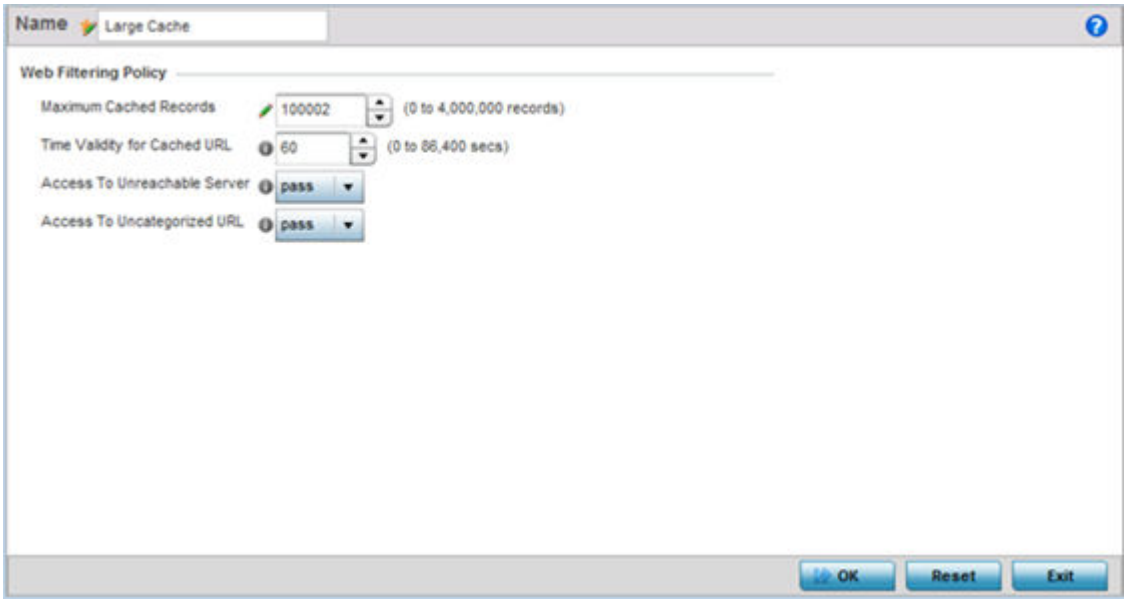
A Web filter policy is a means of managing the number of records and time cached URLs are retained. When configured and applied, the policy also determines whether to filter access to a cached URL when a categorization server is unreachable or is unable to classify request types. To review existing Web filter policies and assess whether new ones require creation, modification or deletion:

1 Select **Configuration → Network → Web Filtering**.




2 Select **Add** to create a new Web filter policy, or select an existing policy and **Edit** to modify its attributes. Obsolete policies can be selected and **Deleted** as needed.

3 If creating a new Web Filtering Policy, assign it a **Name** up to 32 characters to distinguish this policy from others with similar attributes. Modify the new Web Filtering Policy parameters and click **OK** to save the policy, **Reset** to revert back to default settings or **Exit** to exit without creating a new Web Filtering Policy.




4 Set the following **Web Filtering Policy** settings:

| | |
|---|---|
| Maximum Cached Records | Set the maximum number of records (from 0 - 4,000,000) for Web content cached locally on this controller or service platform. The default setting is 100,000 records. |
| Time Validity for Cached URL | Set the maximum amount of a time, from 0 - 86,400 seconds, a URL is valid in the controller or service platform cache. Consider the bandwidth depletion if caching a large number of records over the maximum permissible time validity. |
| Access to Unreachable Server | Either pass or block (filter) access to a cached URL when the categorization server is unreachable. Access is allowed by default. |
| Access to Uncategorized URL | Either pass or block (filter) access to a cached URL when the categorization server fails to classify a request type. Access is allowed by default. |

5 Select **OK** to save the changes to the Web filter policy. Select **Exit** to close the screen without saving the updates.

## Network Deployment Considerations

Before defining a L2TPV3 configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- In respect to L2TP V3, data transfers on the pseudowire can start as soon as session establishment corresponding to the pseudowire is complete.
- In respect to L2TP V3, the control connection keep-alive mechanism of L2TP V3 can serve as a monitoring mechanism for the pseudowires associated with a control connection.

# 9 Security Configuration



When taking precautions to secure wireless traffic between a client and an access point, the network administrator should not lose sight of the security solution in its entirety, because the network's chain is as weak as its weakest link. A WiNG-managed wireless network provides seamless data protection and user validation to protect and secure data at each vulnerable point in the network.

WiNG-managed wireless devices support a Layer 2 wired/wireless firewall and *Wireless Intrusion Protection System* (WIPS) capabilities at the WLAN. They are additionally strengthened with a premium multi-vendor overlay security solution from Air Defense with 24x7 dedicated protection. This security is offered at the most granular level, with role-and location-based secure access available to users based on identity and on the security posture of the client device.

When addressing the security of a WiNG-managed wireless network, consider each of the following:

- Wireless Firewall on page 730
- Configuring IP Firewall Rules on page 744
- Wireless Client Roles on page 753
- Device Fingerprinting on page 762
- Configuring MAC Firewall Rules on page 769
- Wireless IPS (WIPS) on page 772
- Device Categorization on page 781
- Security Deployment Considerations on page 784

## Wireless Firewall

A Firewall enforces access control and is considered a first line of defense in protecting proprietary information within the access-point managed network. The means by which this is accomplished varies, but in principle, a Firewall can be thought of as mechanisms both *blocking* and *permitting* data traffic in the network. Because firewalls implement uniquely defined access control policies, they are of little value unless you have a clear idea of what kind of access to allow or deny. In such an instance, in fact, a firewall could provide a false sense of security.

With WiNG access points, firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing managed wireless clients. Well designed

firewalls block traffic from outside the network while permitting authorized users to communicate freely outside the network.

Firewalls can be implemented in both hardware and software, or a combination of both. All traffic entering or leaving a controller, service platform, or access point passes through the firewall, which examines each message and blocks those not do not meet the security criteria (rules) defined.

Firewall rules define the traffic permitted or denied within the network. Rules are processed by a firewall supported device from first to last. When a rule matches the network traffic that a controller, service platform, or accesspoint is processing, the firewall uses that rule's action to determine whether to allow or deny the traffic.

Rules have two parts:

- A *condition* describes a traffic packet stream. It defines constraints on source and destination devices, the service (protocols and ports), and the incoming interface.
- An *action* describes what happens to packets matching the conditions that have been set. For example, if the packet stream meets all conditions, then traffic is permitted, authenticated, and sent to the destination device.

Additionally, IP and MAC rule-based firewall filtering can be deployed to apply firewall policies to traffic bridged by centrally managed radios. IP and MAC filtering permits or restricts traffic exchanged between hosts, hosts residing on separate WLANs, or hosts forwarding traffic to wired devices.

## Defining a Firewall Configuration

The Wireless Firewall screen has Denial of Service, Storm Control, and Advanced Settings tabs used to create the single firewall policy used by the access point and its connected devices. The Denial of Service tab displays by default.

A *denial of service* (DoS) attack is an attempt to make a computer or network resource unavailable to its intended users. Although the means to carry out a DoS attack will vary, it generally consists of a concerted effort of one or more persons attempting to prevent a device, site or service from functioning temporarily or indefinitely.

Most DoS attacks involve saturating the target device with external communications requests so it cannot respond to legitimate traffic or respond so slowly the device becomes unavailable in respect to its defined data rate. DoS attacks are implemented by either forcing targeted devices to reset or consuming the device’s resources so it can no longer provide service.

To configure a firewall:

1 Got o **Configuration → Security → Wireless Firewall** .

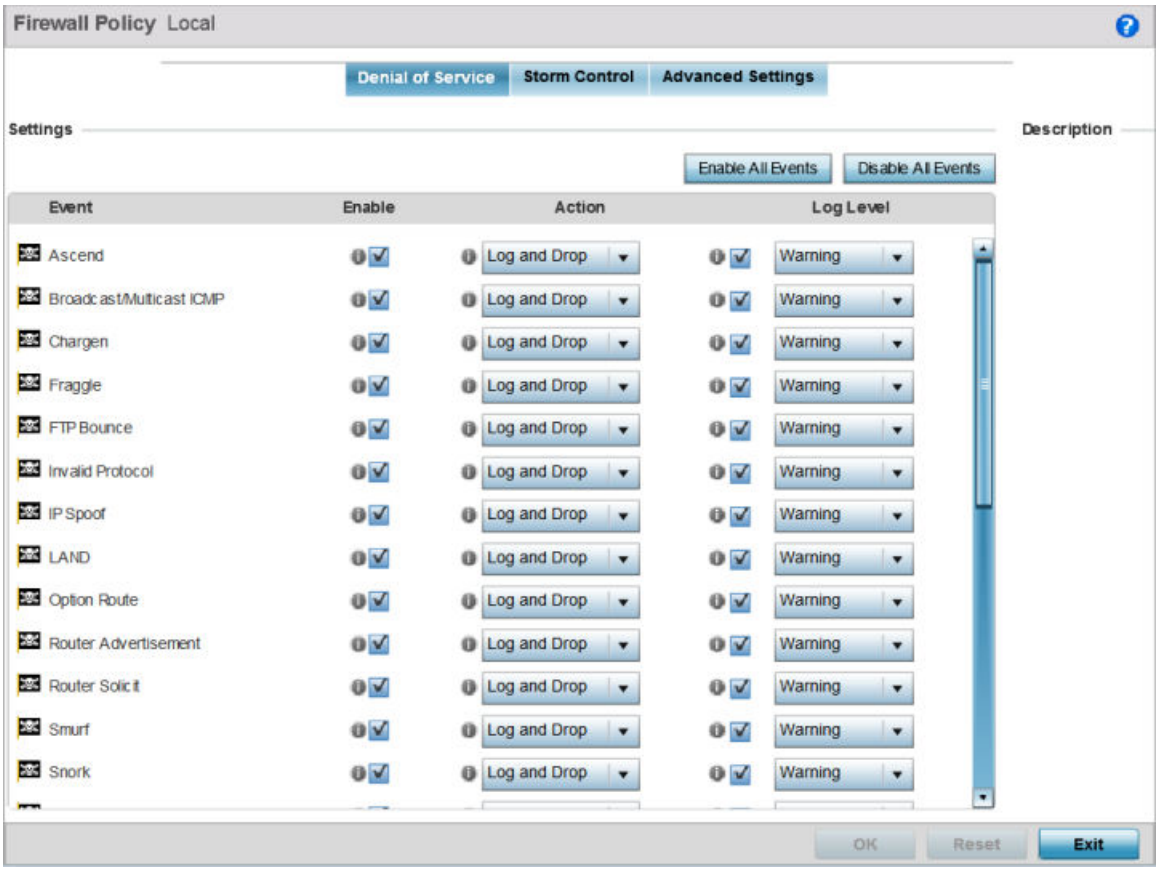



**Figure 339: Wireless Firewall Screen - Denial of Service Tab**

2 Select the **Activate Firewall Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration.

Ensure that this option stays selected to apply the configuration to the access point profile.

The **Settings** field lists all of the DoS attacks for which the firewall has filters. Each DoS filter contains the following four items:

| | |
|---|---|
| Event | Lists the name of each DoS attack. |
| Enable | Select **Enable** to set the firewall to filter the associated DoS attack based on the selection in the Action column. |
| Action | If a DoS filter is enabled, choose an action from the drop-down menu to determine how the firewall policy treats the associated DoS attack.<br>• Log and Drop - An entry for the associated DoS attack is added to the log and then the packets are dropped.<br>• Log Only - An entry for the associated DoS attack is added to the log. No further action is taken.<br>• Drop Only - The DoS packets are dropped. No further action is taken. |
| Log Level | Select this option to enable logging to the system log. Then select a standard Syslog level from the **Log Level** drop-down menu. |

3 The following **Events** can be filtered on behalf of the firewall:

| | |
|---|---|
| Ascend | The Ascend DoS attacks are a series of attacks that target known vulnerabilities in various versions of Ascend routers. |
| Broadcast/Multicast ICMP | Broadcast or Multicast ICMP DoS attacks are a series of attacks that take advantage of ICMP behavior in response to echo replies. These usually involve spoofing the source address of the target and sending ICMP broadcast or multicast echo requests to the rest of the network and in the process flooding the target machine with replies. |
| Chargen | The Chargen attack establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services. |
| Fraggle | The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic. |
| FTP Bounce | The FTP Bounce DoS attack uses a vulnerability in the FTP "PORT" command as a way to scan ports on a target machine by using another machine in the middle. |
| Invalid Protocol | Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, called hijacking, or a DoS attack. |
| IP Spoof | IP Spoof is a category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker. |
| LAND | The LAND DoS attack sends spoofed packets containing the SYN flag to the target destination using the target port and IP address as both the source and destination. This will either crash the target system or result in high resource utilization slowing down all other processes. |
| Option Route | Enables the IP Option Route denial of service check in the firewall. |
| Router Advertisement | In this attack, the attacker uses ICMP to redirect the network router function to some other host. If that host can not provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions). |

| | |
|---|---|
| Router Solicit | The ICMP Router Solicitation scan is used to actively find routers on a network. Of course, a hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network.<br>ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122).<br>By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests. |
| Smurf | The Smurf DoS Attack sends ICMP echo requests to a list of broadcast addresses in a row, and then repeats the requests, thus flooding the network. |
| Snork | The Snork DoS attack uses UDP packet broadcasts to consume network and system resources. |
| TCP Bad Sequence | Enables a TCP Bad Sequence denial of service check in the firewall. |
| TCP FIN Scan | Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the Finish (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting.<br>If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply. |

| | |
|---|---|
| TCP Intercept | A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection.<br>Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing email, using FTP service, and so on.<br>The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.<br>When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt. |
| TCP/IP TTL Zero | The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a Time To Live (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload. |
| TCP Null Scan | Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings.<br>If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply. |
| TCP Post SYN | A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an Intrusion Detection System (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS. |
| TCP Packet Sequence | An attempt to predict the sequence number used to identify packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number used by the sending host. If successful, they can send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may originate from some third host controlled by the attacker. |

| | |
|---|---|
| TCP XMAS Scan | The TCP XMAS Scan floods the target system with TCP packets including the FIN, URG, and PUSH flags. This is used to determine details about the target system and can crash a system. |
| TCP Header Fragment | Enables the TCP Header Fragment denial of service check in the firewall. |
| Twinge | The Twinge DoS attack sends ICMP packets and cycles through using all ICMP types and codes. This can crash some Windows systems. |
| UDP Short Header | Enables the UDP Short Header denial of service check in the firewall. |
| WINNUKE | The WINNUKE DoS attack sends a large amount of data to UDP port 137 to crash the NETBIOS service on windows and can also result on high CPU utilization on the target machine. |
| Hop Limit Zero | Enables the check for Hop Limit in IPv6 packets. If the value is zero, it is considered a DoS and is blocked. |
| Multicast ICMPv6 | The Multicast ICMPv6 attack sends multicast ICMPv6 packets. This is applicable to only ICMPv6 Echo request/reply packets. |
| TCP Intercept Mobility | Enables the detection of IPv6 TCP packets with mobility option Home-Address-Option (HAO) or RH (Routing Header) type two and does not generate TCP syn cookies for these packets. |

4 Select **OK** to update the Denial of Service settings.

Select **Reset** to revert to the last saved configuration. The firewall policy can be invoked at any point in the configuration process by selecting **Activate Firewall Policy** from the upper left-hand side of the access point user interface.

*Firewall Policy Storm Control*

The firewall maintains a facility to control packet storms. Storms are packet bombardments that exceed the high threshold value configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the RF Domain manager interface. Thresholds are configured in terms of packets per second.

To define a storm control configuration for a Firewall policy:

1 Select the Storm Control tab from the Firewall Policy configuration page.

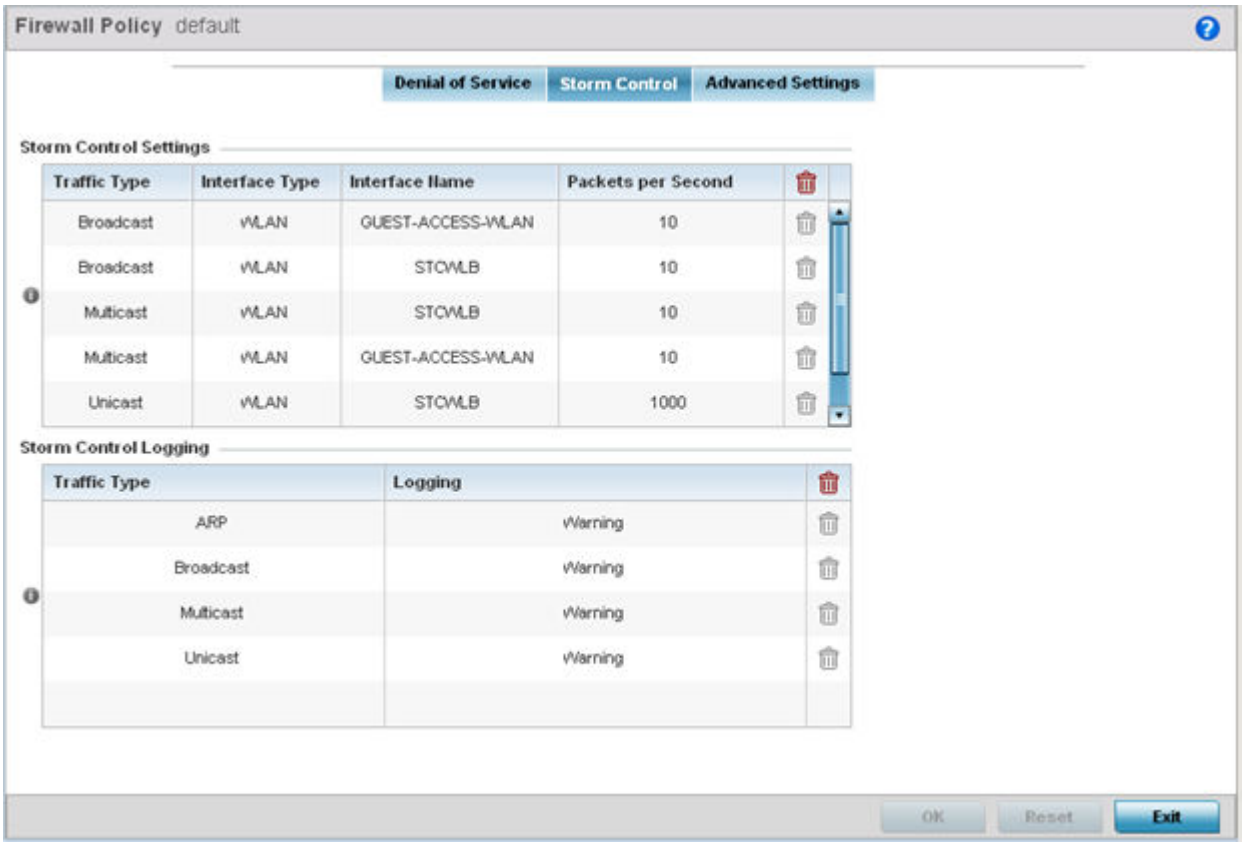



**Figure 340: Wireless Firewall - Add/Edit - Storm Control Screen**

2 Refer to the Storm Control Settings field to set the following:

| | |
|---|---|
| Traffic Type | Use the drop-down menu to define the traffic type for which the Storm Control configuration applies. Options include ARP, Broadcast, Multicast and Unicast. |
| Interface Type | Use the drop-down menu to define the interface for which the Storm Control configuration is applied. Only the specified interface uses the defined filtering criteria. Options include Ethernet, WLAN and Port Channel. |
| Interface Name | Use the drop-down menu to refine the interface selection to a specific WLAN or physical port. This helps with threshold configuration for potentially impacted interfaces. |
| Packets per Second | Select the check box to activate the spinner control used for specifying the packets per second threshold for activating the Storm Control mechanism. |

3 Select **+ Add Row** as needed to add additional Storm Control configurations for other traffic types or interfaces.

Select the **Delete** icon as required to remove selected rows.

4 Refer to the Storm Control Logging field to define how storm events are logged.

| | |
|---|---|
| Traffic Type | Use the drop-down menu to define the traffic type for which the Storm Control logging configuration applies. Options include ARP, Broadcast, Multicast and Unicast. |
| Logging | Select the check box to activate the spinner control used for specifying the standard log level used if a Storm Control attack is detected. The default log level is Warning. |

5 Select **+ Add Row** as needed to add additional Storm Control log entries for other interfaces.

Select the **Delete** icon as required to remove selected rows.

6 Select **OK** to update the Storm Control settings.

Select **Reset** to revert to the last saved configuration.

*Firewall Policy Advanced Settings*

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery (ND) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. Use the Advanced Settings tab to define common IPv4 settings and settings unique to an IPv6 firewall.

To define a firewall policy advanced settings:

1 Select the **Advanced Settings** tab.

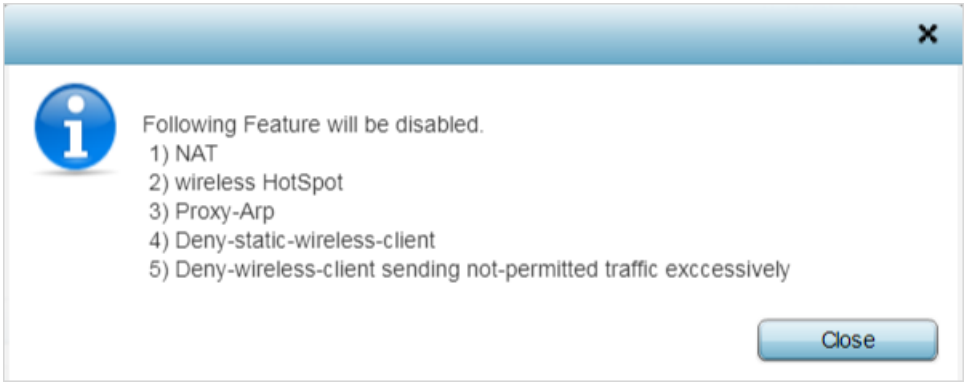
The Common tab is displayed by default.


**Figure 341: Wireless Firewall - Add/Edit - Advanced Settings - Common Tab**

2 Use the **Firewall Status** radio buttons to either enable or disable the firewall policy.

The firewall is enabled by default.

If you disable the firewall, the following message is displayed:



3 Refer to the General field to enable or disable the following firewall configuration parameters:

| | |
|---|---|
| Enable Proxy ARP | Select this check box to allow the Firewall Policy to use Proxy ARP responses for this policy on behalf of another device. Proxy ARP allows the firewall to handle ARP routing requests for devices behind the firewall. This feature is enabled by default. |
| DHCP Broadcast to Unicast | Select this check box to enable the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This feature is disabled by default. |
| L2 Stateful Packet Inspection | Select the check box to enable stateful packet inspection for RF Domain manager routed interfaces within the Layer 2 firewall. This feature is disabled by default. |
| IPMAC Conflict Enable | When multiple devices on the network have the same IP or MAC address this can create routing issues for traffic being passed through the firewall. To avoid these issues, enable Conflict Detection to enable IP and MAC conflict detection. This feature is disabled by default. |
| IPMAC Conflict Logging | Select this option to enable logging for IP and MAC address conflict detection. This feature is disabled by default. |
| IPMAC Conflict Action | Use the drop-down menu to set the action taken when an attack is detected. Options include Log Only, Drop Only or Log and Drop. The default setting is Log and Drop. |
| IPMAC Routing Conflict Enable | Select this option to enable IPMAC Routing Conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct router-mac-address. |
| IPMAC Routing Conflict Logging | Select enable logging for IPMAC Routing Conflict detection. This feature is disabled by default. |
| IPMAC Routing Conflict Action | Use the drop-down menu to set the action taken when an attack is detected. Options include Log Only, Drop Only or Log and Drop. The default setting is Log and Drop. |
| DNS Snoop Entry Timeout | Select this option and set a timeout, in seconds, for DNS Snoop Entry. DNS Snoop Entry stores information such as Client to IP Address and Client to Default Gateway(s) and uses this information to detect if the client is sending routed packets to a wrong MAC address. |
| IP TCP Adjust MSS | Select this option and adjust the value for the maximum segment size (MSS) for TCP segments on the router. Set a value between 472 bytes and 1,460 bytes to adjust the MSS segment size. The default value is 472 bytes. |
| TCP MSS Clamping | Select this option to enable TCP MSS Clamping. TCP MSS Clamping allows for the configuration of the maximum segment size of packets at a global level. |
| Max Fragments/Datagram | Set a value for the maximum number of fragments (between 2 and 8,129) allowed in a datagram before it is dropped. The default value is 140 fragments. |
| Max Defragmentations/Host | Set a value for the maximum number of defragmentations, between 1 and 16,384 allowed per host before it is dropped. The default value is 8. |
| Min Length Required | Select this option and set a minimum length, between 8 bytes and 1,500 bytes, to enforce a minimum packet size before being subject to fragment based attack prevention. |

| | |
|---|---|
| Virtual Defragmentation | Select this option to enable IPv4 and IPv6 virtual defragmentation to help prevent fragment based attacks, such as tiny fragments or large number of fragments. |
| Virtual Defragmentation Timeout | Set a virtual defragmentation timeout from 1- 60 seconds applicable to both IPv4 and IPv6 packets. |

4 Refer to the **Firewall Enhanced Logging** field to set the following parameters:

| | |
|---|---|
| Log Dropped ICMP Packets | Use the drop-down menu to define how dropped ICMP packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include Rate Limited, All or None. The default setting is None. |
| Log Dropped Malformed Packets | Use the drop-down menu to define how dropped malformed packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include Rate Limited, All or None. The default setting is None. |
| Enable Verbose Logging | Check this box to enable verbose logging mode for the firewall. |

5 The firewall policy allows traffic filtering at the application layer using the Application Layer Gateway feature.

The Application Layer Gateway provides filters for the following common protocols:

| | |
|---|---|
| FTP ALG | Select this option to allow FTP traffic through the firewall using its default ports. This feature is enabled by default. |
| TFTP ALG | Select this option to allow TFTP traffic through the firewall using its default ports. This feature is enabled by default. |
| PPTP ALG | Select this option to allow PPTP traffic through the firewall using its default ports. The *Point-to-Point Tunneling Protocol* (PPTP) is a network protocol that enables the secure transfer of data from a remote client to an enterprise server by creating a VPN across TCP/IP-based data networks. PPTP encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. This feature is enabled by default. |
| SIP ALG | Select this option to allow SIP traffic through the firewall using its default ports. This feature is enabled by default. |
| SCCP ALG | Select this option to allow SCCP traffic through the firewall using its default ports. This feature is enabled by default. |
| Facetime ALG | Select this option to allow Facetime traffic through the firewall using its default ports. This feature is enabled by default. |
| DNS ALG | Select this option to allow DNS traffic through the firewall using its default ports. This feature is enabled by default. |

6 Select the **Enable Stateful DHCP Checks** check box to enable the stateful checks of DHCP packet traffic through the firewall.

The default setting is enabled. When enabled, all DHCP traffic flows are inspected.

7 Define **Flow Timeout** intervals for the following flow types impacting the firewall:

| | |
|---|---|
| TCP Close Wait | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 10 seconds. |
| TCP Established | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 90 minutes. |

| | |
|---|---|
| TCP Reset | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 10 seconds. |
| TCP Setup | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 10 seconds. |
| Stateless TCP Flow | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 90 seconds. |
| Stateless FIN/RESET Flow | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 10 seconds. |
| ICMP | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 30 seconds. |
| UDP | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 30 seconds. |
| Any Other Flow | Define a flow timeout value in either **Seconds** (1 - 32,400), **Minutes** (1 - 540) or **Hours** (1 - 9). The default setting is 30 seconds. |

8 Refer to the **TCP Protocol Checks** field to set the following parameters:

| | |
|---|---|
| Check TCP states where a SYN packet tears down the flow | Select the check box to allow a SYN packet to delete an old flow in TCP_FIN_FIN_STATE and TCP_CLOSED_STATE and create a new flow. The default setting is enabled. |
| Check unnecessary resends of TCP packets | Select the check box to enable the checking of unnecessary resends of TCP packets. The default setting is enabled. |
| Check Sequence Number in ICMP Unreachable error packets | Select the check box to enable sequence number checks in ICMP unreachable error packets when an established TCP flow is aborted. The default setting is enabled. |
| Check Acknowledgment Number in RST packets | Select the check box to enable the checking of the acknowledgment number in RST packets which aborts a TCP flow in the SYN state. The default setting is enabled. |
| Check Sequence Number in RST packets | Select the check box to check the sequence number in RST packets which abort an established TCP flow. The default setting is enabled. |

9 Select **OK** to update the firewall policy's advanced common settings.

Select **Reset** to revert to the last saved configuration.

### Firewall Policy IPv6 Settings

Use the **Advanced Settings** → **IPv6 Settings** tab to define settings unique to an IPv6 firewall.

1 Select the **IPv6 Settings** tab.

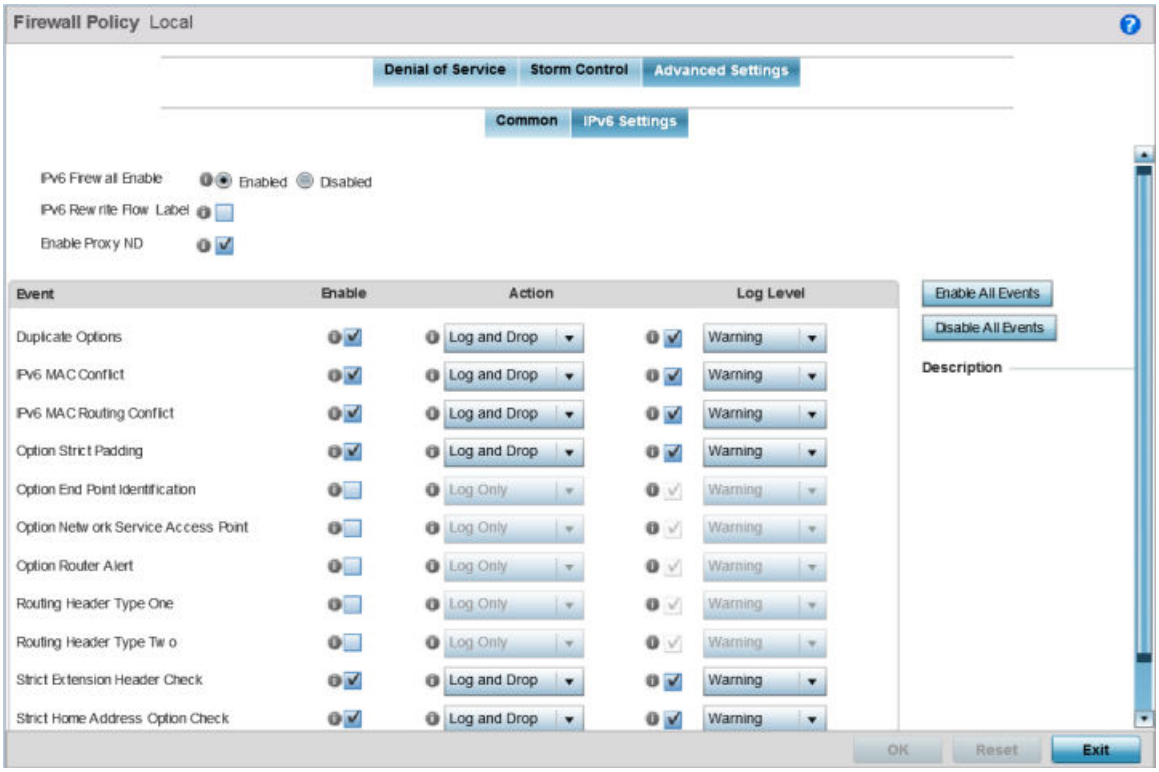



**Figure 342: Wireless Firewall - Add/Edit - Advanced Settings - IPv6 Settings Tab**

2 Refer to the **IPv6 Firewall Enable** option to provide firewall support to IPv6 packet streams.

This setting is enabled by default. Disabling IPv6 firewall support also disables proxy neighbor discovery.

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery (ND) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed uniquely of eight groups of four hexadecimal digits separated by colons.

3 Select **IPv6 Rewrite Flow Label** to provide flow label rewrites for each IPv6 packet.

A flow is a sequence of packets from a particular source to a particular (unicast or multicast) destination. The flow label helps keep packet streams from looking like one massive flow. Flow label rewrites are disabled by default and must be manually enabled.

Flow label re-writes enable the re-classification of packets belonging to a specific flow. The flow label does nothing to eliminate the need for packet filtering. This setting is disabled by default.

4 Select **Enable Proxy ND** to generate neighbor discovery responses on behalf of another controller, service platform or Access Point managed device.

When enabled, any IPv6 packet received on an interface is parsed to see whether it is known to be a neighbor solicitation. This setting is enabled by default.

5 Use the **Event** table to enable individual IPv6 unique events.

IPv6 events can be individually enabled or collectively enabled/disabled using the **Enable All Events** and **Disable All Events** buttons. The Description area displays a brief description of the selected event.

| | |
|---|---|
| Event | The **Event** column lists the name of each IPv6 specific event subject to logging. |
| Enable | Checking **Enable** sets the firewall policy to filter the associated IPv6 event based on the selection in the Action column. |
| Action | If a filter is enabled, chose an action from the drop-down menu to determine how the firewall treats the associated IPv6 event.<br>• Log and Drop - An entry for the associated IPv6 event is added to the log and then the packets are dropped.<br>• Log Only - An entry for the associated IPv6 event is added to the log. No further action is taken.<br>• Drop Only - The packet is dropped. No further action is taken. |
| Log Level | To enable logging to the system log, check the box in the **Log Level** column. Then select a standard Syslog level from the **Log Level** drop-down menu. |

6 Select **OK** to update the firewall policy's advanced IPv6 settings.

Select **Reset** to revert to the last saved configuration.

## Configuring IP Firewall Rules

IP-based firewalls function like *Access Control Lists* (ACLs) to filter or mark packets, as opposed to filtering packets on Layer 2 ports.

IP-based Firewall rules are specific to *source* and *destination* IP addresses and the unique *rules* and *precedence* definitions assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying an IP ACL. Firewall rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

Note
Once defined, a set of IP firewall rules must be applied to an interface to be a functional filtering tool.

There are separate policy creation mechanisms for IPv4 and IPv6 traffic. With both IPv4 and IPv6, f you intend tto deny specific types of packets, we recommend that you create access rules for traffic entering a controller, service platform, or access point interface before the controller, service platform, or access point spends time processing them. This is because access rules are processed before other types of firewall rules.

IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

For more information, see:


- Setting an IPv4 or IPv6 Firewall Policy on page 745
- Setting an IP SNMP ACL Policy on page 749
- Setting a Network Group Alias on page 750
- Setting a Network Service Alias on page 752

## Setting an IPv4 or IPv6 Firewall Policy

Before defining a firewall configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective.

To add or edit an IP based Firewall Rule policy:

1 Select **Configuration** > **Security**.

2 Select **IPv4 ACL** or **IPv6 ACL** to display existing IP forewall policies.

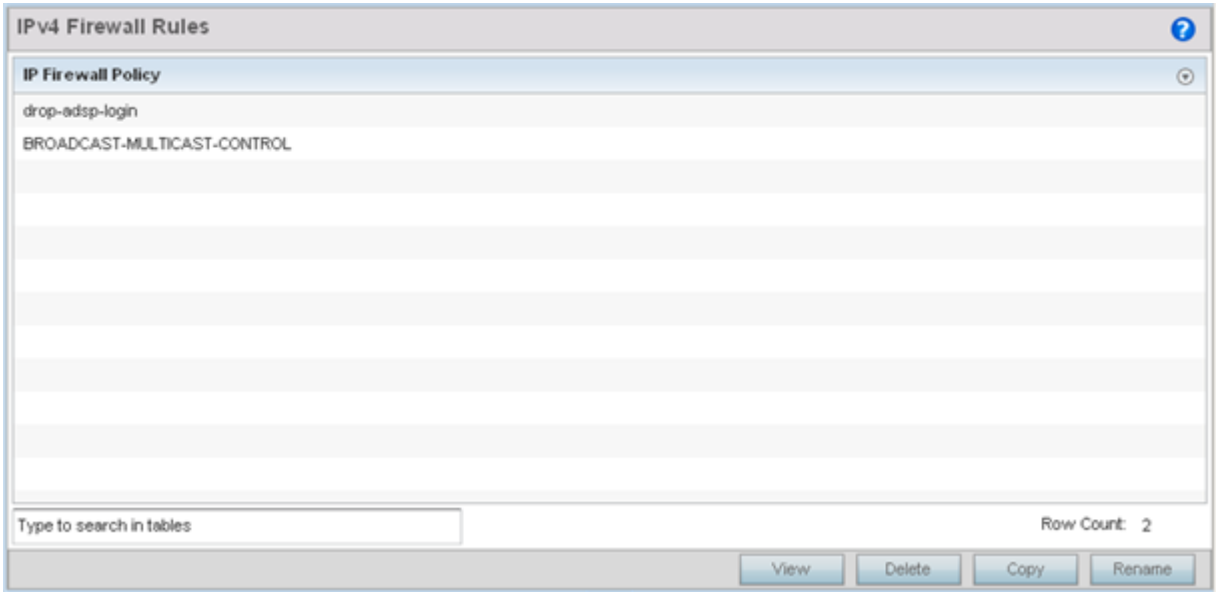



**Figure 343: IP Firewall Policy Screen**

3 Select **Add** to create a new IPv4 or IPv6 firewall rule.

Select an existing policy and click **Edit** to modify the attributes of that policy's configuration.

4 Select the added row to expand it into configurable parameters for a new rule.

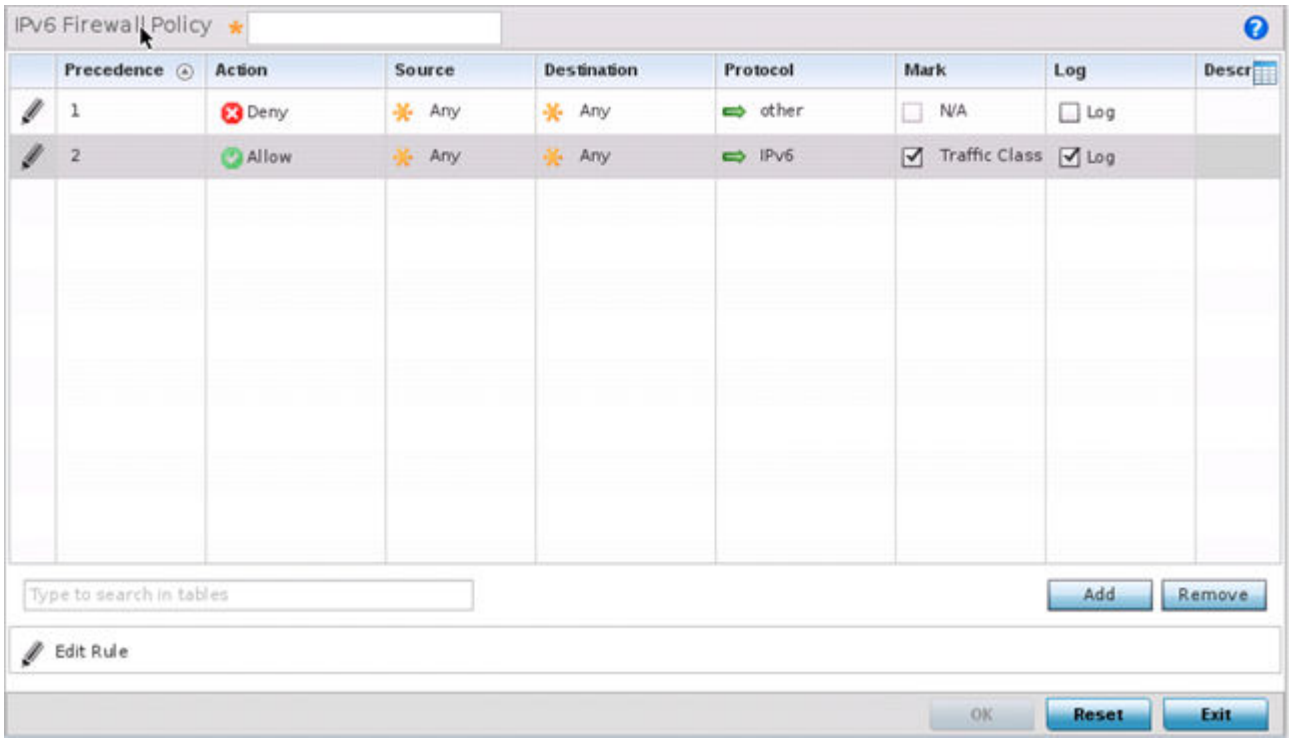



**Figure 344: IP Firewall Rules Screen - Adding a New Rule**

If adding a new rule, enter a name up to 32 characters.

5 Select **Add** to add a new firewall rule.

IP firewall configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

a Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.

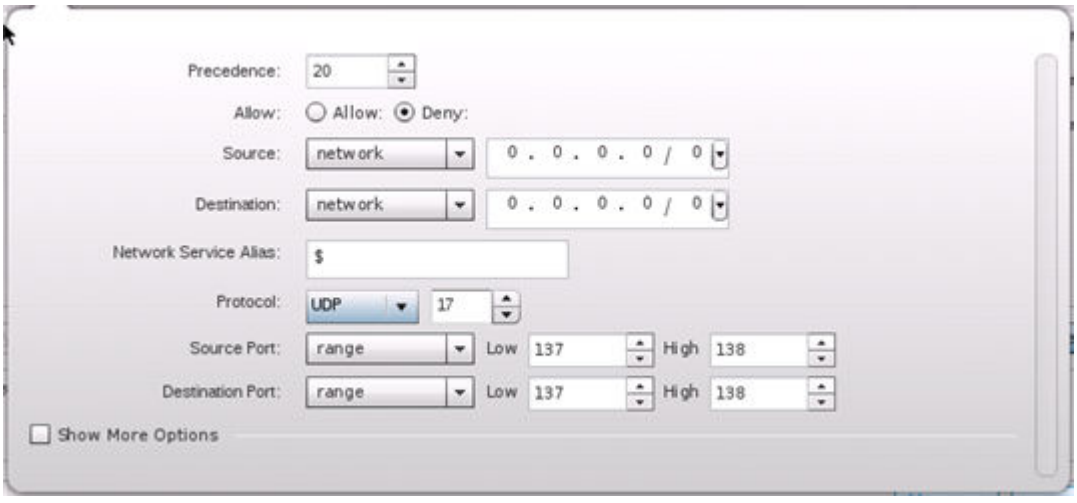



**Figure 345: WLAN Security - IP Firewall Rules - Edit Rule Screen**

b Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.


**Figure 346: WLAN Security - IP Firewall Rules - Add Criteria Pop-up**

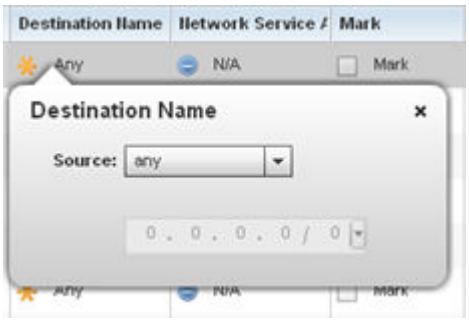



**Figure 347: IWLAN Security - IP Firewall Rules - Add/Edit Specific Criteria Pop-up**

Note
Only those selected IP ACL filter attributes display. Each value can have its current setting adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

6 Define the following IP firewall rule settings as required:

| | |
|---|---|
| Precedence | Specify or modify a precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority. |
| Action | Every IP Firewall rule is made up of matching criteria rules. The action defines the packet's disposition if it matches the specified criteria. The following actions are supported:<br>• Deny - Instructs the firewall to restrict a packet from proceeding to its destination.<br>• Permit - Instructs the firewall to allow a packet to proceed to its destination. |

| | |
|---|---|
| Source | Select the source for creating the ACL. Source options include:<br>• Any - Indicates any host device in any network.<br>• Network – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network.<br>• Host – Indicates a single host with a specific IP address.<br>• Alias – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL. |
| Destination | Select the destination for creating the ACL. Destination options include:<br>• Any - Indicates any host device in any network.<br>• Network – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network.<br>• Host – Indicates a single host with a specific IP address.<br>• Alias – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL. |
| Protocol | Set a service alias as a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant. |
| Network Service Alias | The service alias is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $ character and containing one special character) and include the protocol as relevant. Selecting either tcp or udp displays an additional set of specific TCP/UDP source and destinations port options. |
| Source Port | If using either tcp or udp as the protocol, define whether the source port for incoming IP ACL rule application is any, equals or an administrator defined range. If not using tcp or udp, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for Low and High numeric range settings. A source port cannot be a destination port. |
| Destination Port | If using either tcp or udp as the protocol, define whether the destination port for incoming IP ACL rule application is any, equals or an administrator defined range. If not using tcp or udp, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for Low and High numeric range settings. |
| ICMP Type | Selecting ICMP as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The Internet Control Message Protocol (ICMP) uses messages identified by numeric type. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10. |
| ICMP Code | Selecting ICMP as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding code, helpful for troubleshooting network issues (0 - Net Unreachable, 1- Host Unreachable, 2 - Protocol Unreachable etc.). |
| Start VLAN | Select a Start VLAN icon within a table row to set (apply) a start VLAN range for this IP ACL filter. The Start VLAN represents the virtual LAN beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply. |

| | |
|---|---|
| End VLAN | Select an End VLAN icon within a table row to set (apply) an end VLAN range for this IP ACL filter. The End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply. |
| Protocol | Select the protocol to filter for this ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number. |
| Mark | Select this option to mark certain fields inside a packet before allowing them. Mark is applicable only for Allow rules. Mark sets the rule's 802.1p or dscp level (from 0 - 7). |
| Log | Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed. |
| Enable | Select this option to enable or disable this particular IP Firewall rule in this rule set. |
| Description | Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a **Select Columns** screen used to add or remove IP ACL criteria from the table. |

7 Select **Add** to add additional IP firewall rule configurations.

Select **Remove** to remove selected IP firewall rules.

8 Select **OK** when completed to update the IP firewall rules.

Select **Reset** to revert to the last saved configuration.

## Setting an IP SNMP ACL Policy

SNMP performs network management functions using a data structure called a *Management Information Base* (MIB). SNMP is widely implemented but not very secure, because it uses only text community strings for accessing controller or service platform configuration files.

Use SNMP ACLs to help reduce SNMP's vulnerabilities, as SNMP traffic can be exploited to produce a denial of service (DoS).

To create an IP SNMP ACL:

1 Select **Configuration** > **Security** > **IP Firewall**.

2 Expand the **IP Firewall** menu item and select **IP SNMP ACL**.

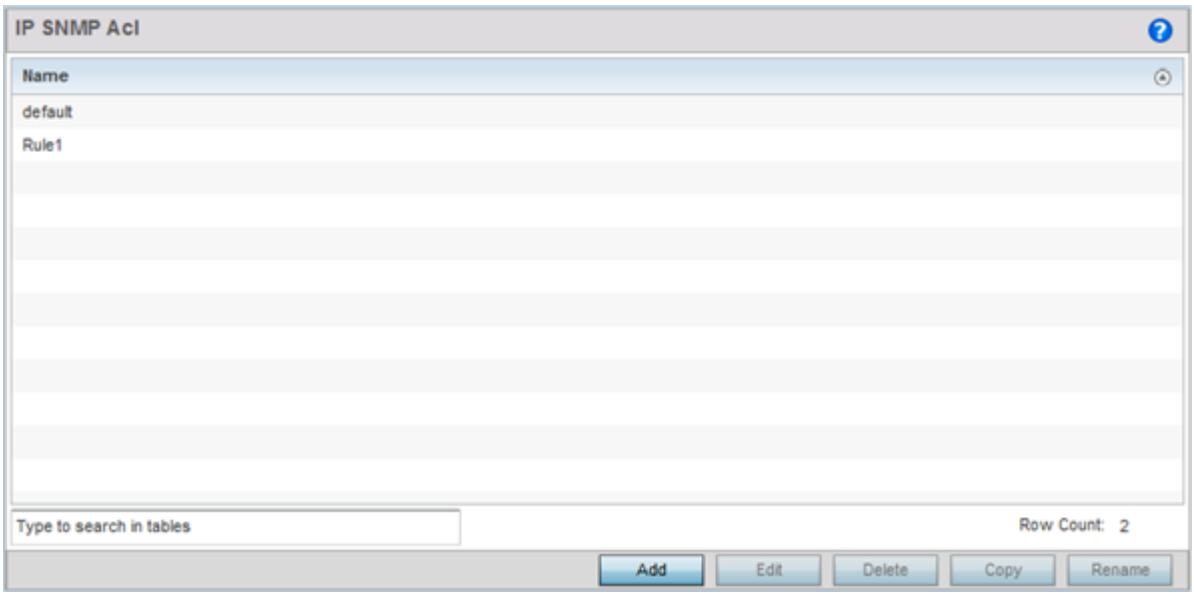



**Figure 348: IP SNMP ACL Screen**

## Setting a Network Group Alias

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

To set a network group alias configuration for an IP firewall:

1 Select **Configuration** > **Security**.

2 Expand the **IP Firewall** menu item and select **Network Group Alias**.

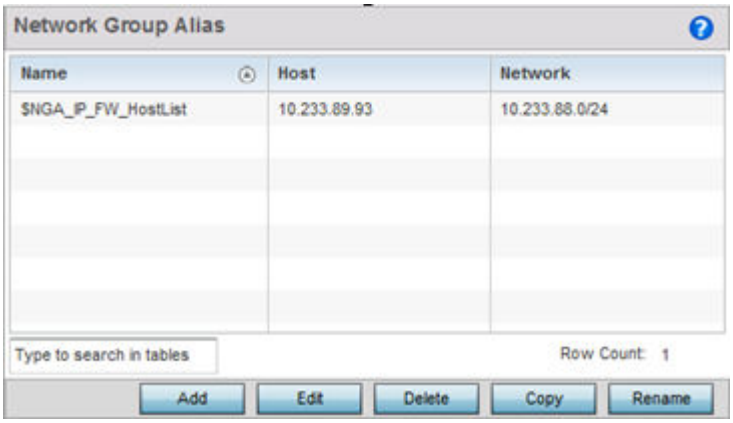



**Figure 349: IP Firewall Network Group Alias Screen**

3 Click **Add** to create a new network group alias.

Select an existing network group alias and click **Edit** to modify it.

4 If you are creating a new network group alias, assign it a **Name** up to 32 characters to distinguish this alias configuration from others with similar attributes.

The network group alias name always starts with a dollar sign ($). Select **Reset** to revert to the last saved configuration. Select **Exit** to exit without creating a network group alias.

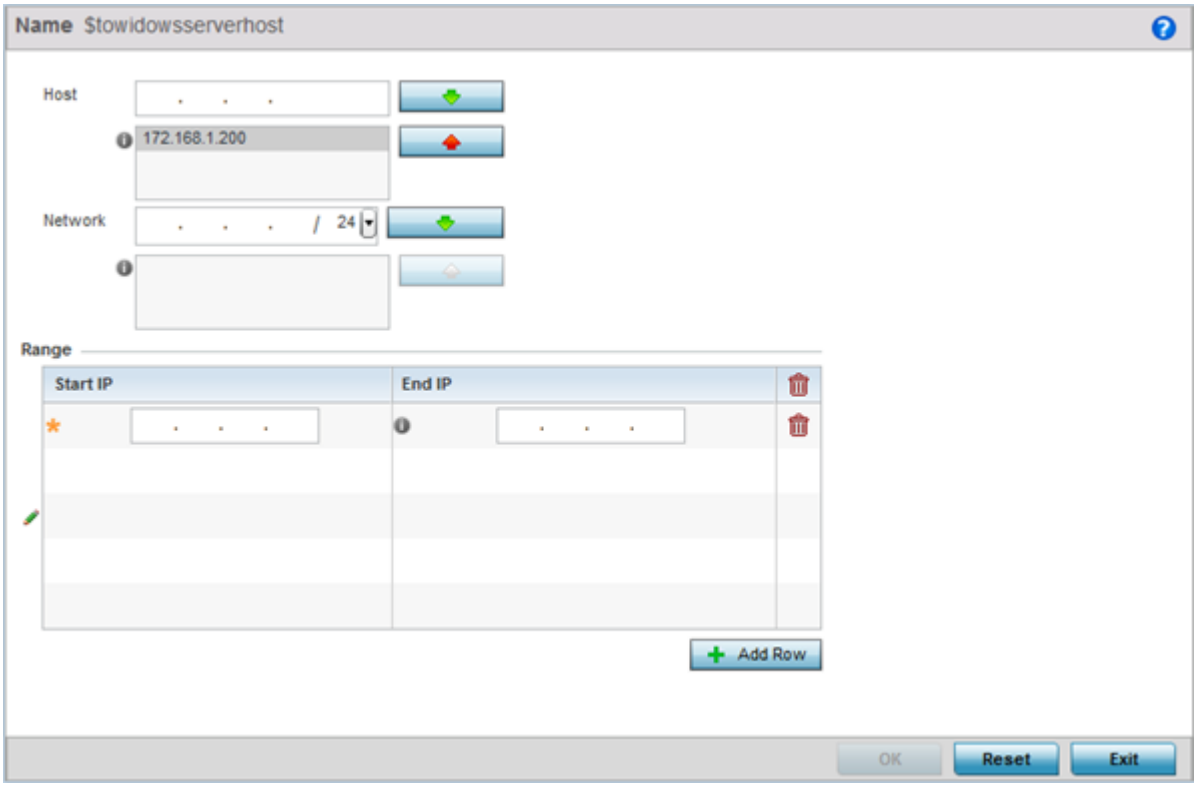



**Figure 350: Network Group Alias Add Screen**

5 Define the following network group alias parameters:

| | |
|---|---|
| Host | Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table. |
| Network | Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table. |

6 Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range, or double-click on an existing alias range entry to edit it.

7 Select **OK** when completed to update the network group alias settings.

Select **Reset** to revert the screen to its last saved configuration.

## Setting a Network Service Alias

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to two source port ranges and up to two destination port ranges can be configured. A maximum of four protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

To define a service alias configuration for an IP firewall:

1 Select **Configuration** > **Security** > **IP Firewall** > **Network Service Alias** from the Web UI.

The Network Service Alias screen displays.

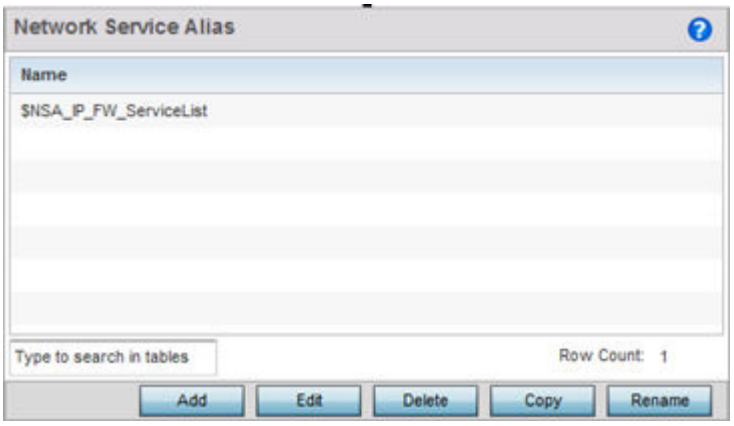



**Figure 351: IP Firewall Network Service Alias Screen**

2 Select **Add** to create a new network service alias.

Select an existing network service alias and click **Edit** to modify it. Select **Delete** to remove an existing network service alias from those available in the list.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

3 If you are adding a new **Network Service Alias**, give it a **Name** up to 32 characters to distinguish this alias configuration from others with similar attributes.

The network group alias name always starts with a dollar sign ($).

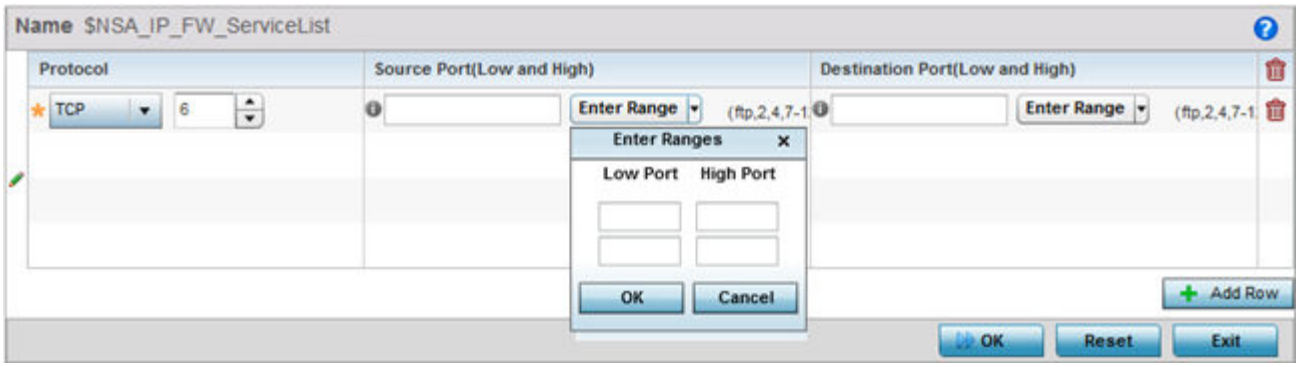



**Figure 352: IP Firewall Network Service Alias - Add/Edit Screen**

Select **Reset** to revert to the last saved configuration. Select **Exit** to exit without creating a network service alias.

4 Select **+ Add Row** and provide the following configuration parameters:

| | |
|---|---|
| Protocol | Specify the protocol for which the alias is created. Use the drop down to select the protocol from eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp and udp. Select **other** if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected. |
| Source Port (Low and High) | This field is relevant only if the protocol is tcp or udp.<br>Specify the source ports for this protocol entry. A range of ports can be specified. Select the **Enter Ranges** button next to the field to enter a lower and higher port range value. Up to eight (8) ranges can be specified. |
| Destination Port (Low and High) | This field is relevant only if the protocol is tcp or udp.<br>Specify the destination ports for this protocol entry. A range of ports can be specified. Select the **Enter Ranges** button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified. |

5 In the **Range** field, use the **+ Add Row** button to specify the Start IP address and End IP address for the service alias range, or double-click on an existing service alias range entry to edit it.

6 Select **OK** when completed to update the network service alias settings.

Select **Reset** to revert the screen to its last saved configuration.

## Wireless Client Roles

Define wireless client roles to filter clients from based on matching policies. Matching policies (much like ACLs) are sequential collections of *permit* and *deny* conditions that apply to packets received from connected clients. When a packet is received from a client, the controller, service platform or access point compares the packet fields against applied matching policy rules to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified, the packet is dropped.

Additionally, wireless client connections are also managed by granting or restricting access by specifying a range of IP or MAC addresses to include or exclude from connectivity. These MAC or IP

access control mechanisms are configured as Firewall Rules to further refine client filter and matching criteria.

## Configuring a Client's Role Policy

To configure a wireless client's role policy and matching criteria:

1 Go to **Configuration → Security → Wireless Client Roles.**

The Wireless Client Roles screen displays the name of those client role policies created thus far.

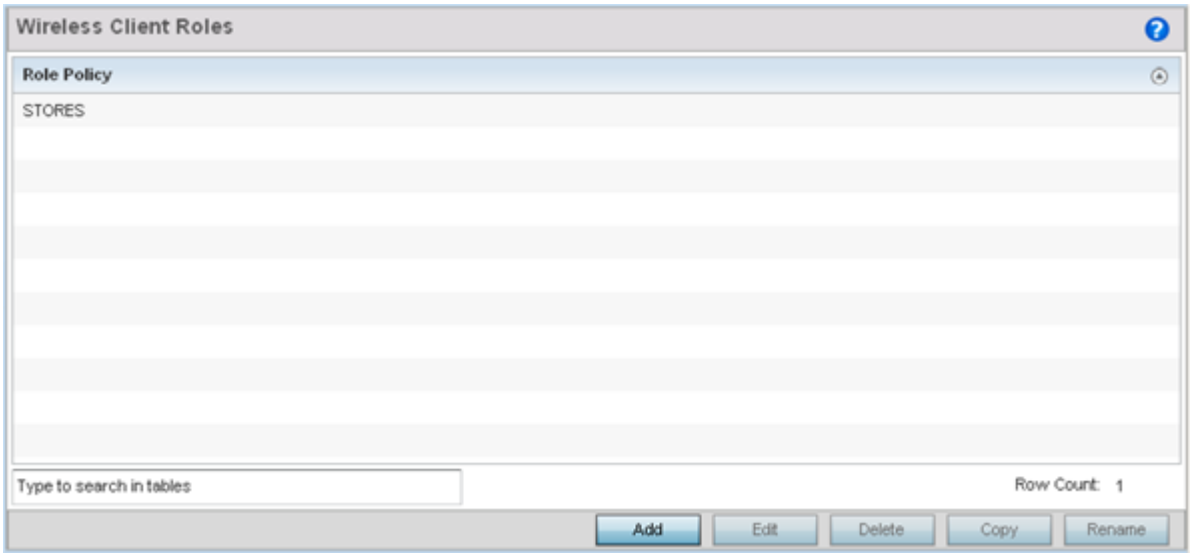



**Figure 353: Wireless Client Roles Screen**

2 Select **Add** to create a new Wireless Client Role policy, **Edit** to modify an existing policy or **Delete** to remove a policy.

The LDAP Settings tab displays by default.

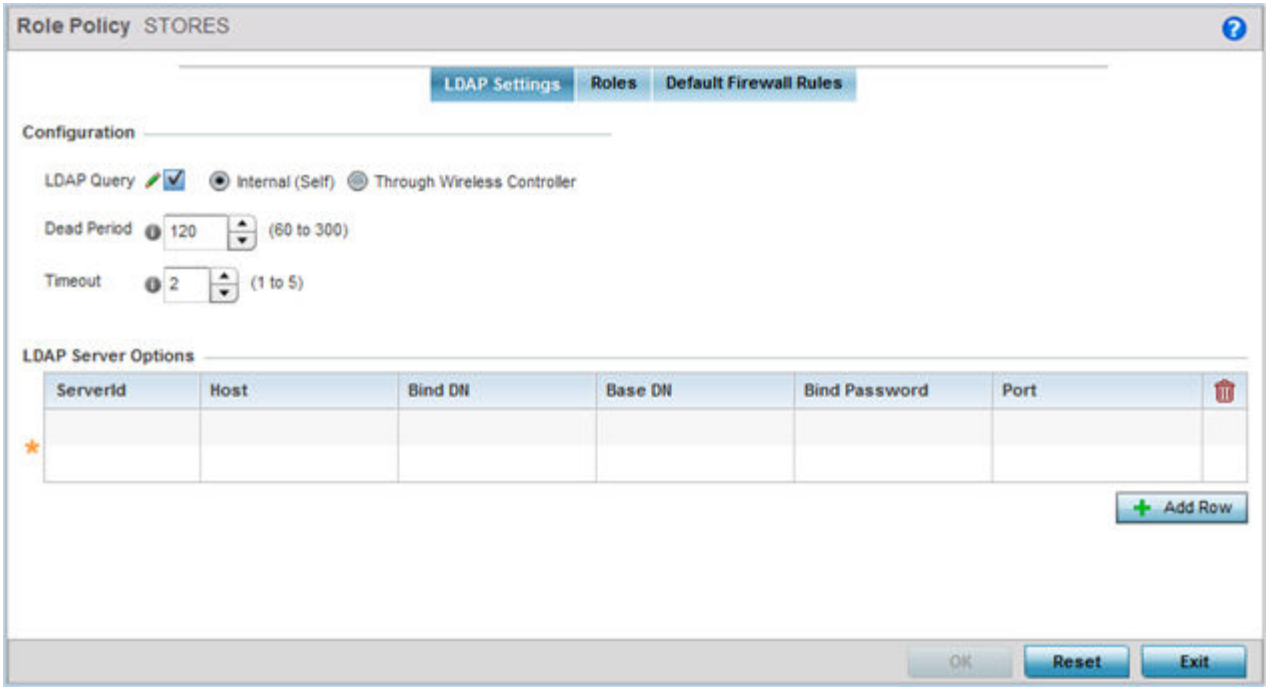



**Figure 354: Wireless Client Roles - Add/Edit - LDAP Settings Tab**

3 In the Configuration section, define the following LDAP server parameters:

| | |
|---|---|
| LDAP Query | If LDAP attributes are enabled for the selected wireless client role policy, select an LDAP query mode of either Internal (Self) or Through Wireless Controller. Select Internal (Self) to use local LDAP server resources configured in the LDAP Server Options. |
| Dead Period | When using an external LDAP server, select the Dead Period between 60 and 300 seconds. The Dead Period is the timeout value before the system will attempt to rebind with the LDAP server. |
| Timeout | When using an external LDAP server, select a Timeout value to specify how long of a delay between request and responses before LDAP bind and queries will be timed out. |

4 In the LDAP Server Options section, use the **+ Add Row** button to add an LDAP server to the list or double-click on an existing LDAP server entry to edit it.

When adding or editing the LDAP server options, define the following parameters:

| | |
|---|---|
| ServerId | When adding or editing an LDAP server entry, enter the LDAP server ID as either 1 or 2. |
| Host | When adding or editing an LDAP server entry, enter the LDAP server's fully qualified domain name or IP address in the **Host** field. |
| Bind DN | When adding or editing an LDAP server entry, enter the LDAP server's bind distinguished name in the **Bind DN** field. |

| | |
|---|---|
| Base DN | When adding or editing an LDAP server entry, enter the LDAP server's base distinguished name in the **Base DN** field. |
| Bind Password | When adding or editing an LDAP server entry, enter the password for bind. Click the **Show** button to display the password. |
| Port | When adding or editing an LDAP server entry, enter the LDAP server port number. To select from a list of frequently used services and their corresponding port numbers, use the drop-down menu and select a service. |

5 Click on the **Roles** tab.

If no policies have been created, a default wireless client role policy can be applied. The Roles screen lists existing policies. Any of these existing policies can be selected and edited or a new role can be added.

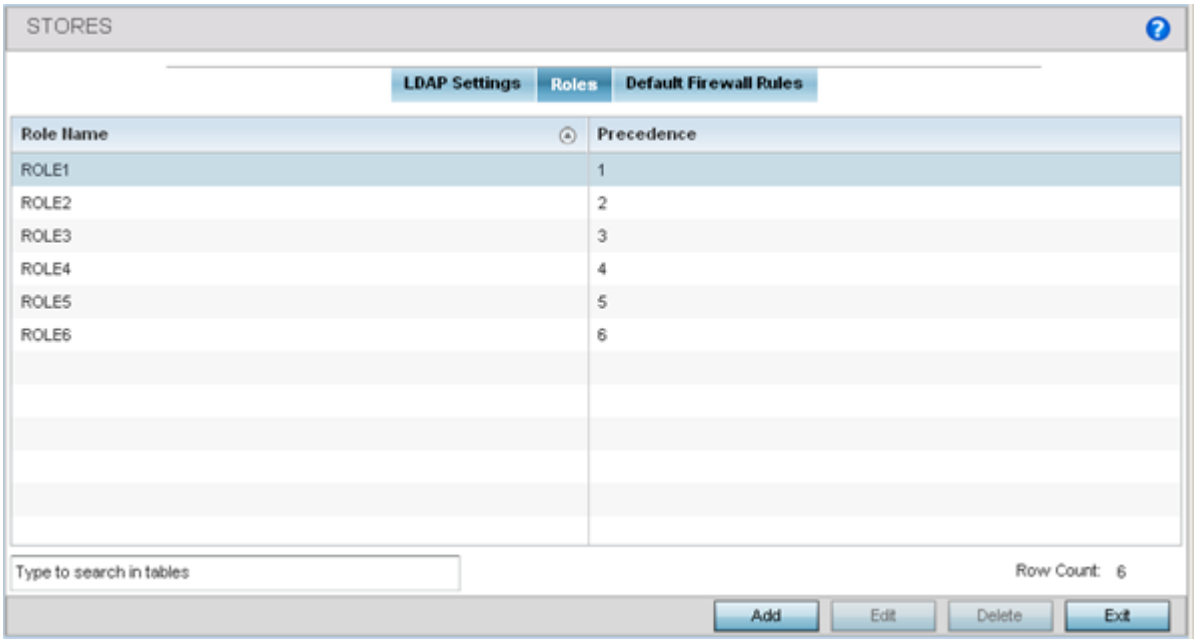



**Figure 355: Wireless Client Roles - Add/Edit - Roles Tab**

6 Refer to the following configuration data for existing roles:

| | |
|---|---|
| Role Name | Displays the name assigned to the client role policy when it was initially created. |
| Precedence | Displays the precedence number associated with each role. Precedence numbers determine the order a role is applied. Roles with lower numbers are applied before those with higher numbers. Precedence numbers are assigned when a role is created or modified, and two or more roles can share the same precedence. |

7 Select **Add** to create a new wireless client role policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

The Role Policy Roles screen displays with the Settings tab displayed by default.

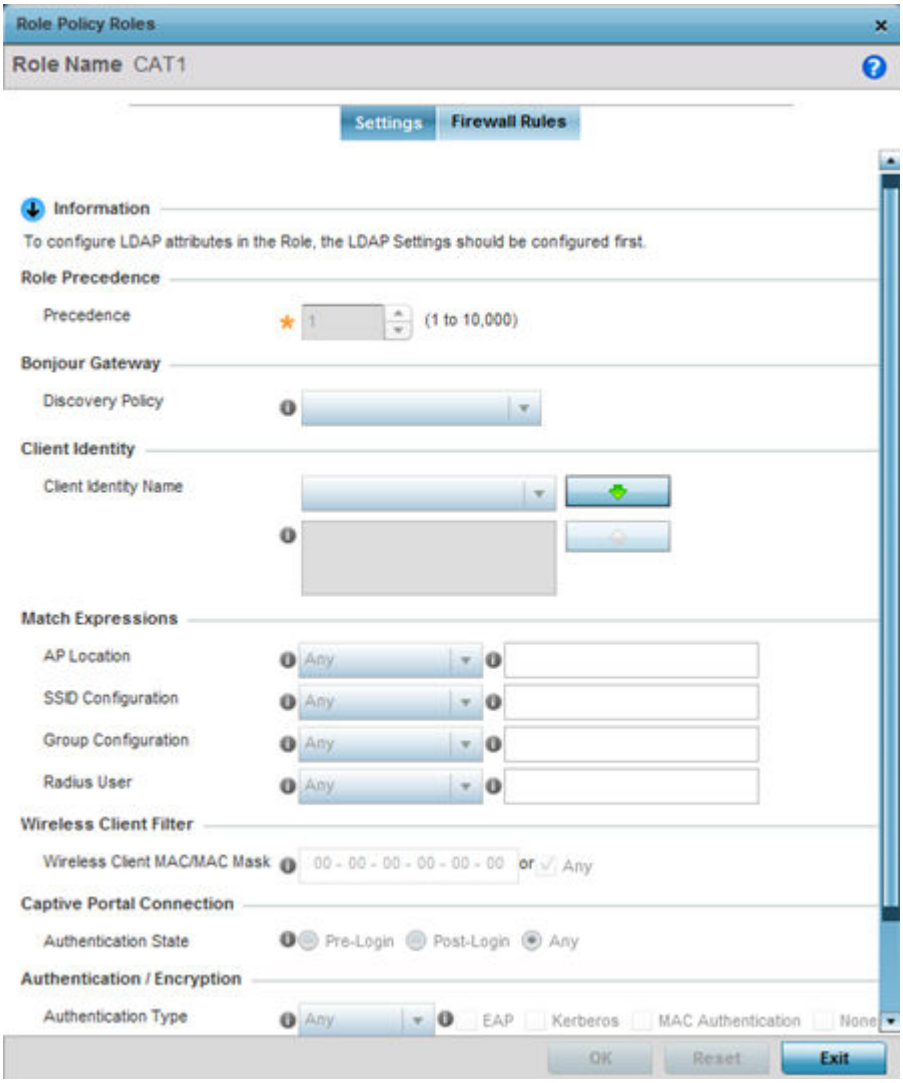



**Figure 356: Wireless Client Roles - Add/Edit - Roles - Settings Tab**

8 If you are creating a new role, assign it a **Role Name** to help differentiate it from others that may have a similar configuration.

The role policy name cannot exceed 64 characters. The name cannot be modified as part of the edit process.

9 In the **Role Precedence** field, use the spinner control to set a numerical precedence value between 1 - 10,000.

Precedence determines the order a role is applied. Roles with lower numbers are applied before those with higher numbers. While there's no default precedence for a role, two or more roles can share the same precedence.

10 Use the **Discovery Policy** drop-down menu to specify the **Bonjour Gateway**.

Bonjour provides a method to discover services on a LAN. Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

Note
The WiNG 7.1 release does not provide support for Bonjour feature on AP505 and AP510 model access points. This feature will be supported in future releases.

11 In the **Client Identity** field, define the client type (Android etc.) used as matching criteria within the client role policy.

Create new client identity types or edit existing ones as required.

12 Refer to the Match Expressions field to create filter rules based on AP locations, SSIDs and RADIUS group memberships.

| | |
|---|---|
| AP Location | Use the drop-down menu to specify the location of an access point matched in an RF domain or the access point's resident configuration. Select one of the following filter options:<br>• Exact - The role is applied only to access points with the exact location string specified in the role.<br>• Contains - The role is applied only to access points whose location contains the location string specified in the role.<br>• Does Not Contain - The role is applied only to access points whose location does not contain the location string specified in the role.<br>• Any - The role is applied to any access point location. This is the default setting. |
| SSID Configuration | Use the drop-down menu to define a wireless client filter option based on how the SSID is specified in a WLAN. Select one of the following options:<br>• Exact - The role is applied only when the exact SSID string is specified in the role..<br>• Contains - The role is applied only when the SSID contains the string specified in the role.<br>• Does Not Contain - The role is applied when the SSID does not contain the string specified in the role.<br>• Any - The role is applied to any SSID Location. This is the default setting. |

| | |
|---|---|
| Group Configuration | Use the drop-down menu to define a wireless client filter option based on how the RADIUS group name matches the provided expression. Select one of the following options:<br>• Exact - The role is applied only when the exact RADIUS Group Name string is specified in the role..<br>• Contains - The role is applied when the RADIUS Group Name contains the string specified in the role.<br>• Does Not Contain - The role is applied when the RADIUS Group Name does not contain the string specified in the role.<br>• Any - The role is applied to any RADIUS Group Name. This is the default setting. |
| RADIUS User | Use the drop-down menu to define a filter option based on how the RADIUS user name (1-255 characters in length) matches the provided expression. Select one of the following options:<br>• Exact - The role is applied only when the exact RADIUS user string is specified in the role..<br>• Contains - The role is applied when the RADIUS user starts with the string specified in the role.<br>• Does Not Contain - The role is applied when the RADIUS user does not contain the string specified in the role.<br>• Any - The role is applied to any RADIUS user name. This is the default setting. |

13 Use the **Wireless Client Filter** parameter to define a wireless client MAC address filter that is applied to each role.

Select the **Any** radio button to use any MAC address. The default is **Any**.

14 Refer to the **Captive Portal Connection** parameter to define when wireless clients are authenticated when making a captive portal authentication request.

Secure guest access is referred to as captive portal. A captive portal is guest access policy for providing temporary and restrictive access to the wireless network. Existing captive portal policies can be applied to a WLAN to provide secure guest access.

15 Select the **Pre-Login** check box to conduct captive portal client authentication before the client is logged.

Select **Post-Login** to have the client share authentication credentials after it has logged into the network. Selecting **Any** (the default setting) makes no distinction on whether authentication is conducted before or after the client has logged in.

16 Use the **Authentication / Encryption** field to set the authentication and encryption filters applied to this wireless client role.

The options for both authentication and encryption are:

| | |
|---|---|
| Equals | The role is applied only when the authentication and encryption type matches the exact method(s) specified by the radio button selections. |
| Not Equals | The role is applied only when the authentication and encryption type does not match the exact method(s) specified by the radio button selections. |
| Any | The role is applied to any type. This is the default setting for both authentication and encryption. |

17 Use the **+** (plus sign) to the left of the LDAP Attributes label to expand it.

Set the following LDAP Attributes for the role policy: The following filter criteria apply to each LDAP attribute:

| | |
|---|---|
| Exact | The role is applied only when the exact string is specified in the role. |
| Contains | The role is applied when the LDAP attribute contains the string specified in the role. |
| Does Not Contain | The role is applied when the LDAP attribute does not contain the string specified in the role. |
| Any | The role is applied to any LDAP attribute. This is the default setting. |

| | |
|---|---|
| City | Enter a 2-31 character name of the city filtered in the role. |
| Company | Enter a 2-31 character name of the organizational company filtered in the role. |
| Country | Enter a 2-31 character name of the country (co) filtered in the role. |
| Department | Enter a 2-31 character name of the organizational department filtered in the role. |
| Email | Enter a 2-31 character name of the Email address filtered in the role. |
| Employee Id | Enter a 2-31 character name of the employee ID filtered in the role. |
| State | Enter a 2-31 character name of the state filtered in the role. |
| Title | Enter a 2-31 character name of the job or organizational title filtered in the role. |
| Member Of | Provide a 64 character maximum description of the group membership in the role. |

18 Select **OK** to update the Settings screen.

Select **Reset** to revert to the last saved configuration.

19 Select the **Firewall Rules** tab to set default Firewall rules for Inbound and Outbound IP and MAC Firewall rules.

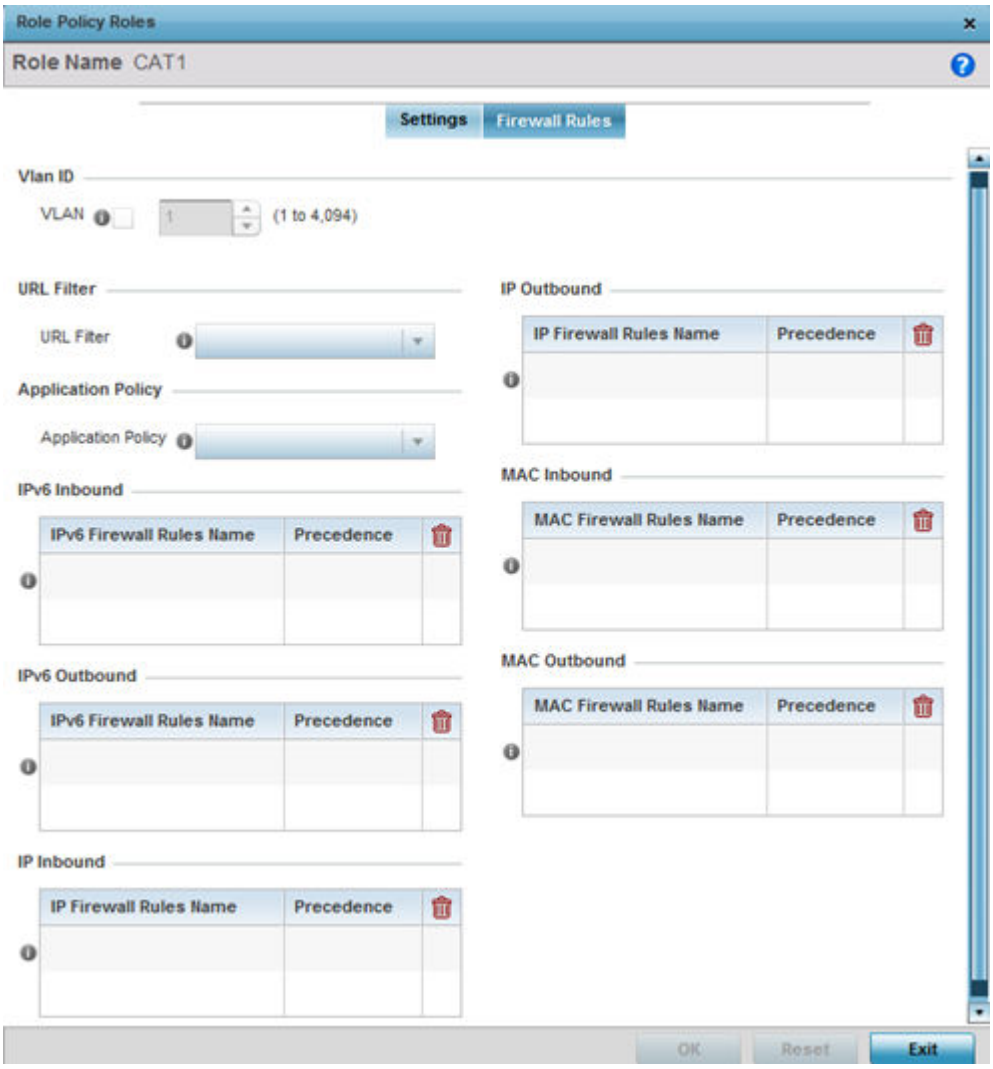



**Figure 357: Wireless Client Roles - Add/Edit - Roles - Firewall Rules Tab**

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic based on inbound and outbound IP and MAC rules.

IP-based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny, or mark designation to packet traffic.

20 Set the **Vlan ID** (from 1 - 4094) for the virtual LAN used by clients matching the IP or MAC inbound and outbound rules of this policy.

21 Use the drop-down to select the appropriate **Application Policy** to use with this firewall rule.

An application policy defines the rules or actions executed on recognized HTTP (Facebook), enterprise (Webex), and peer-to-peer (gaming) applications or application-categories.

22 Specify an **IPv6 Inbound** or **IPv6 Outbound** firewall rule by selecting a rule from the drop-down menu and use the spinner control to assign the rule Precedence.

Rules with lower precedence are always applied first to packets. Select the **+ Add Row** button or **Delete** icon as needed to add or remove IPv6 firewall rules. If no IPv6 Inbound or Outbound firewall ACL exist create the IPv6 firewall ACL and use here.

23 Specify an **IP Inbound** or **IP Outbound** firewall rule by selecting a rule from the drop-down menu and use the spinner control to assign the rule Precedence.

Rules with lower precedence are always applied first to packets. Select the **+ Add Row** button or **Delete** icon as needed to add or remove IP firewall rules. If no IP Inbound or Outbound firewall ACL exist create the IP firewall ACL and use here.

24 Specify an **MAC Inbound** or **MAC Outbound** firewall rule by selecting a rule from the drop-down menu and use the spinner control to assign the rule Precedence.

Rules with lower precedence are always applied first to packets. Select the **+ Add Row** button or **Delete** icon as needed to add or remove MAC firewall rules. If no MAC Inbound or Outbound firewall ACL exist create the MAC firewall ACL and use here.

25 Select **OK** to save the Firewall Rules updates.

Select **Reset** to revert to the last saved configuration.

## Device Fingerprinting

With an increase in *Bring Your Own Device* (BYOD) corporate networks, there's a parallel increase in the number of possible attack scenarios within the network. BYOD devices are inherently unsafe, as the organization's security mechanisms do not extend to these personal devices deployed in the corporate wireless network. Organizations can protect their networks by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting enables administrators to control how BYOD devices access the network and to control their access permissions.

Note
Ensure that DHCP is enabled on the WLAN on which device fingerprinting is to be enabled.

Note
The WiNG 7.1 release does not support device fingerprinting on AP505 and AP510 model access points. This feature will be supported in future releases.

To configure device fingerprinting:

1 Go to **Configuration → Security → Device Fingerprinting** .

The Client Identity screen displays.

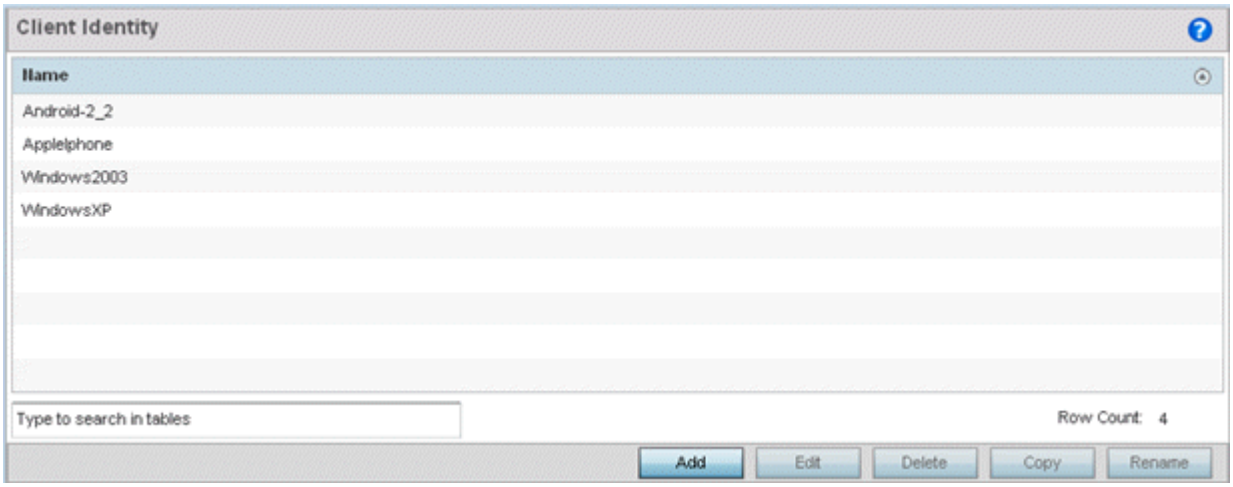



**Figure 358: Security - Device Fingerprinting - Client Identity Screen**

2 Select **Add** to create a new client identity policy.

Client identity policies configure the signatures used to identify clients and then use these signatures to classify and assign permissions to them. A set of pre-defined client identities are included.

Click **Edit** to modify a selected policy, or **Delete** to remove obsolete policies from the list of those available.

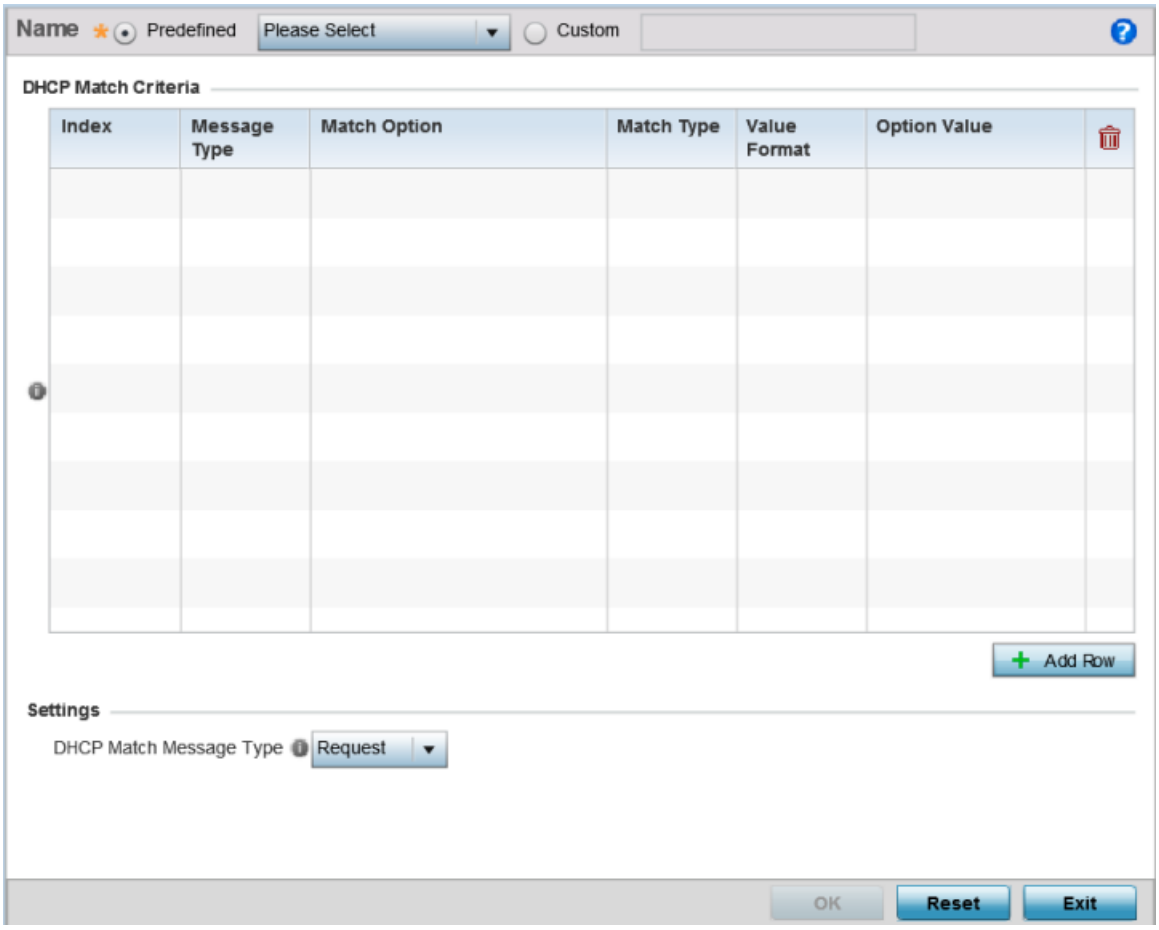



**Figure 359: Security - Device Fingerprinting - New Client Identity Screen**

3 Select **Pre-defined** and use the drop-down menu to select from a list of pre-defined client identities.

Once a client identity is selected from the drop-down menu, the **DHCP Match Criteria** field is populated with the fingerprints for the selected client identity

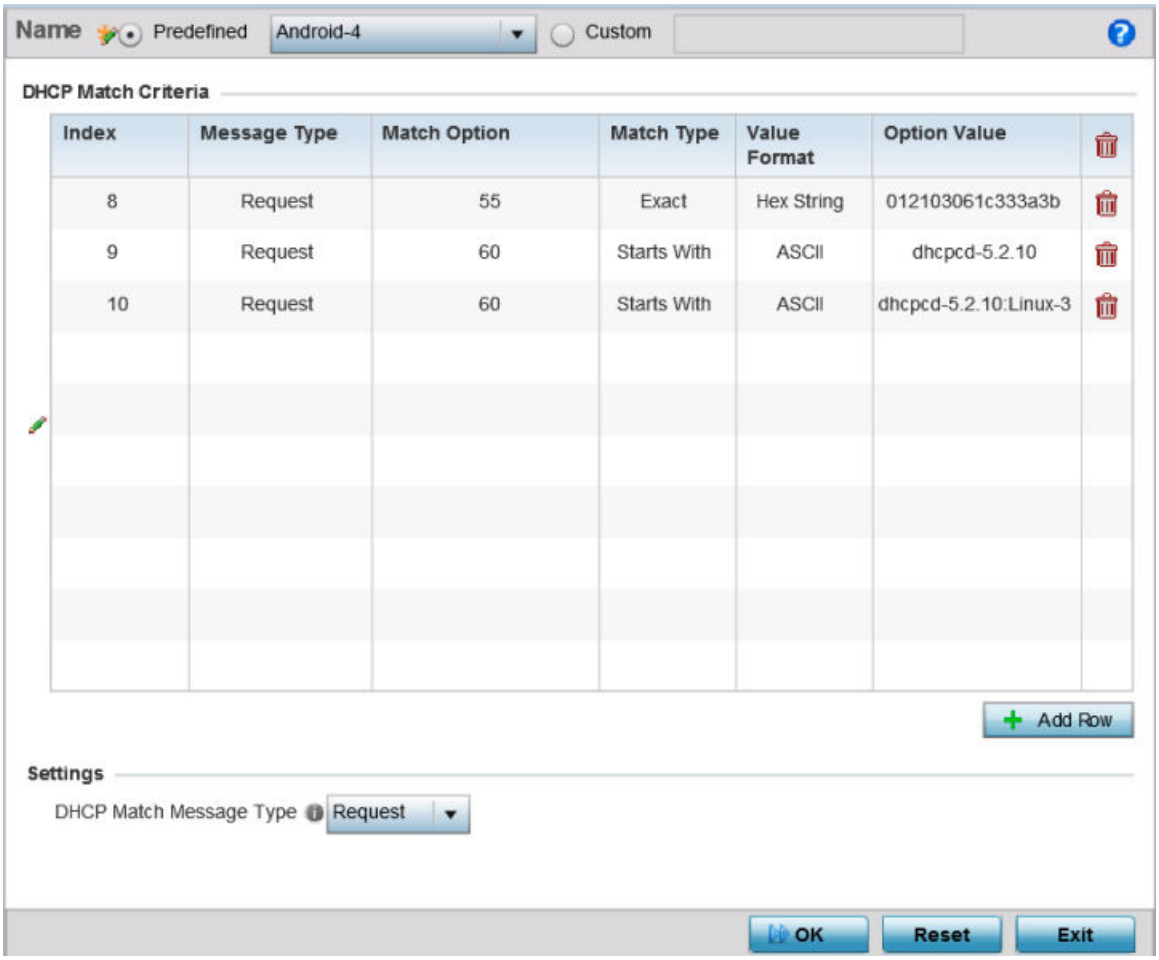



**Figure 360: Security - Device Fingerprinting - New Client Identity - Pr-Defined Identity Screen**

4 To create a custom client identity, select **Custom** and provide a name in the adjacent field.

Click the **OK** button at the bottom of the screen.

5 From the **DHCP Match Message Type** drop-down menu, select the message type to match.

The available options are **`request`**, **`discover`**, **`any`**, and **`all`**. Use this option to select the message type on which the fingerprint is matched.

| | |
|---|---|
| request | Indicates the fingerprint is only checked with any DHCP request message received from any device. |
| discover | Indicates the fingerprint is only checked with any DHCP discover message received from any device. |
| any | Indicates the fingerprint is checked with either the DHCP request or the DHCP discover message. |
| all | Indicates the fingerprint is checked with both the DHCP request and DHCP discover message. |

6 Click **Add Row** to add a new signature to include in the client identity.

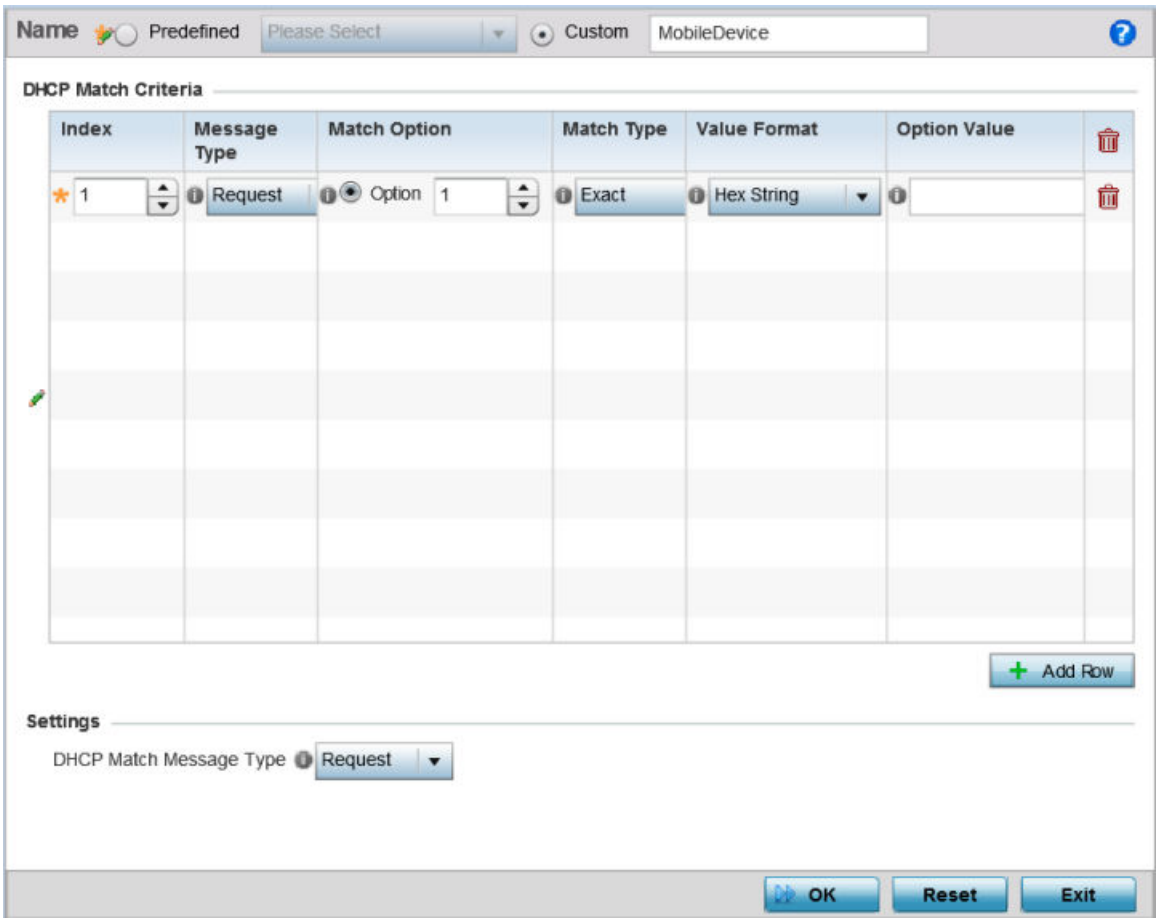



**Figure 361: Security - Device Fingerprinting - Client Signature Screen**

7 Provide the following information for each device signature:

| | |
|---|---|
| Index | Use the spinner control to assign an index for this signature. A maximum of 16 signatures can be created in each client identity. |
| Message Type | Use the drop-down menu to designate the DHCP message in which to look for the signatures.<br>• Request – Looks for a signature in DHCP request messages.<br>• Discover – Looks for a signature in DHCP discover messages. |
| Match Option | The **Match Option** field contains the following options:<br>• Option Codes – Indicates that the Option Codes passed in the DHCP request/ discover message are used for matching.<br><br>Options are passed in the DHCP discover/request messages as Option Code, Option Type, Option Value sets. When Option Codes is selected, all the Option Code passed in the DHCP discover/request are extracted and a fingerprint is derived. This derived fingerprint is used to identify the device.<br>• Option – Indicates that a specific DHCP Option is used to identify the device. When this option is selected, a text box is enabled to input the DHCP Option that is used for fingerprinting. |

| | |
|---|---|
| Match Type | Use the drop-down menu to select how the signatures are matched. Available options include:<br>• Exact – The complete signature string matches the string specified in the Option Value field.<br>• Starts With – The signature is checked if it starts with the string specified in the Option Value field.<br>• Contains – The signature is checked if it contains the string specified in the Option Value field. |
| Value Format | Use the drop-down menu to select the character format of the value that is being checked. The value can be either **ASCII** or **Hexa String**. |
| Option Value | Use this text box to set the 64-character maximum DHCP option value to match. |

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

Select **Reset** to revert all changes made to this screen.

Click **Exit** to close the Client Identity screen.

9 From the main menu on the left, select **Client Identity Group**.

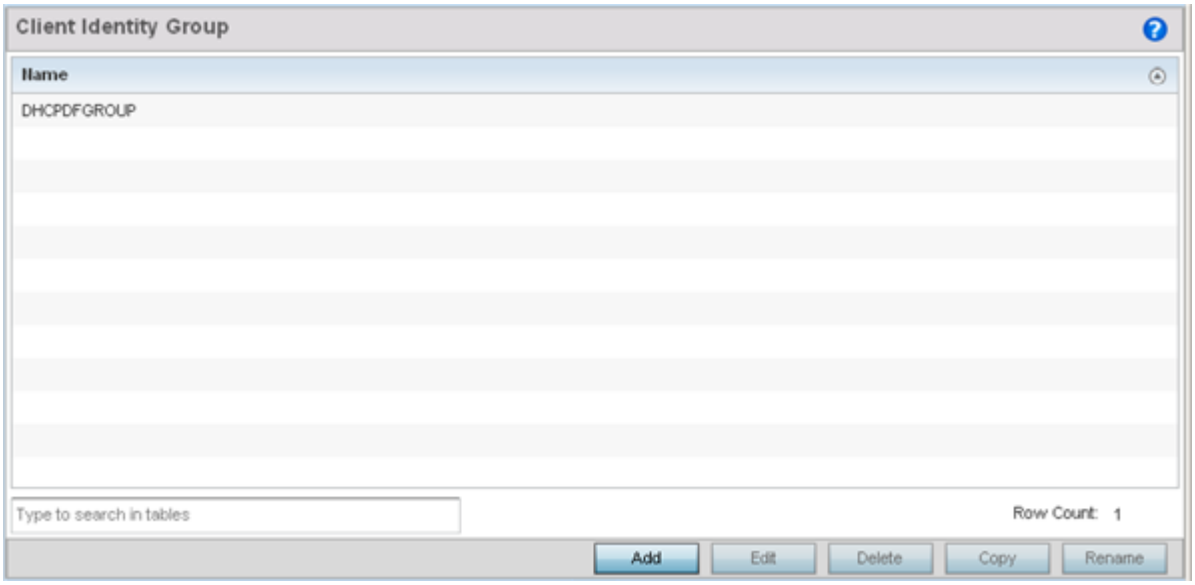



**Figure 362: Security - Device Fingerprinting - Client Identity Group**

A *Client identity group* is a collection of client identities. Each client identity included in a client identity group is set a priority value that indicates the priority for that identity when device fingerprinting.

Device fingerprinting relies on specific information sent by a client when acquiring an IP address and configuration information from a DHCP server. Device fingerprinting uses the DHCP options sent by the wireless client in DHCP request or discover packets to derive a unique signature specific to a device class. For example, Apple devices have a different signature from Android devices. This unique signature is used to classify the devices and assign permissions and restrictions on each class.

10 Select **Add** to create a new Client Identity Group policy.

Client Identity Group policies configure the signatures used to identify clients and then use these signatures to classify and assign permissions to them.

Click **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

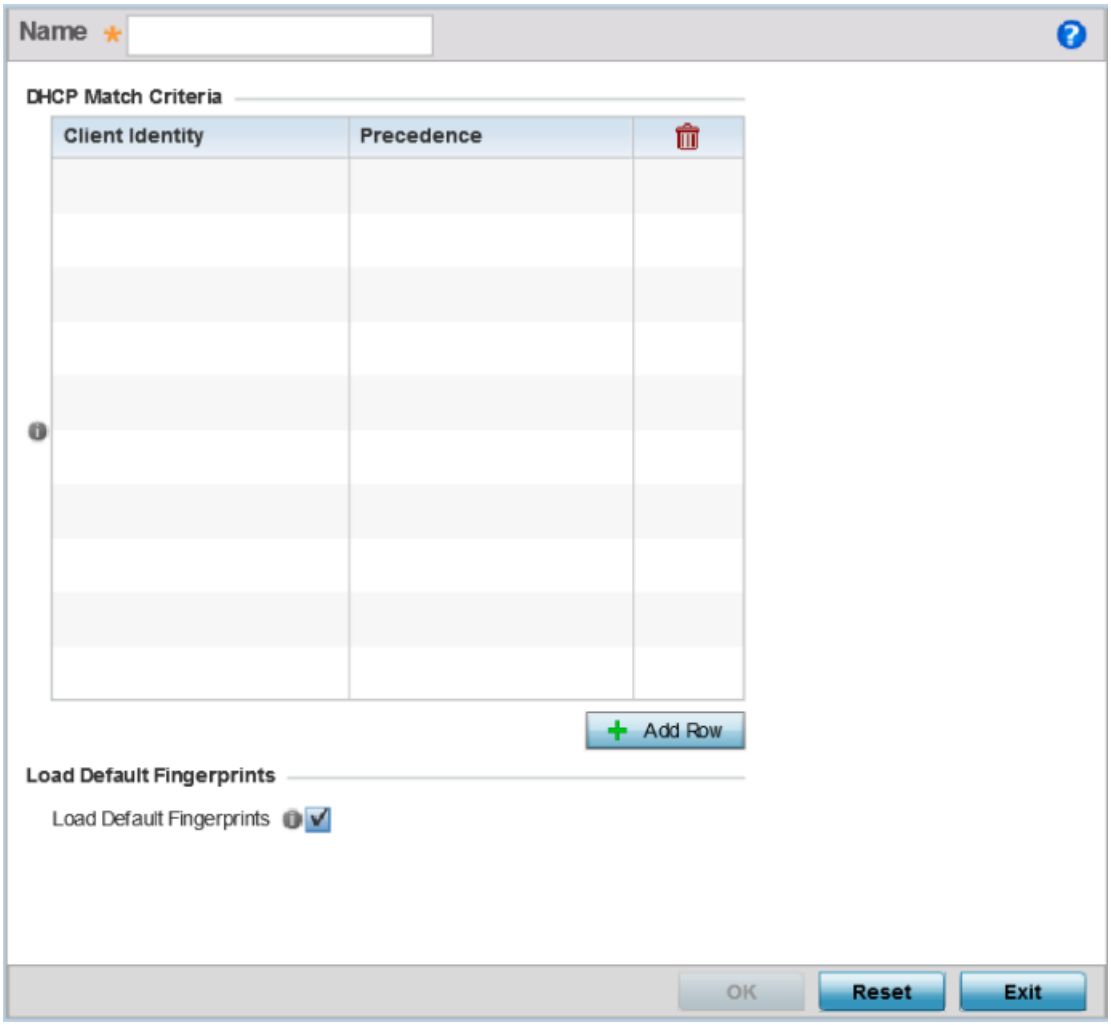



**Figure 363: Security - Device Fingerprinting - Client Identity Group - New Client Identity Group**

11 Provide a name in the **Name** field for the new client identity and click **OK** at the bottom of the screen.

12 Click **Add Row** to add a new signature included in the client identity.

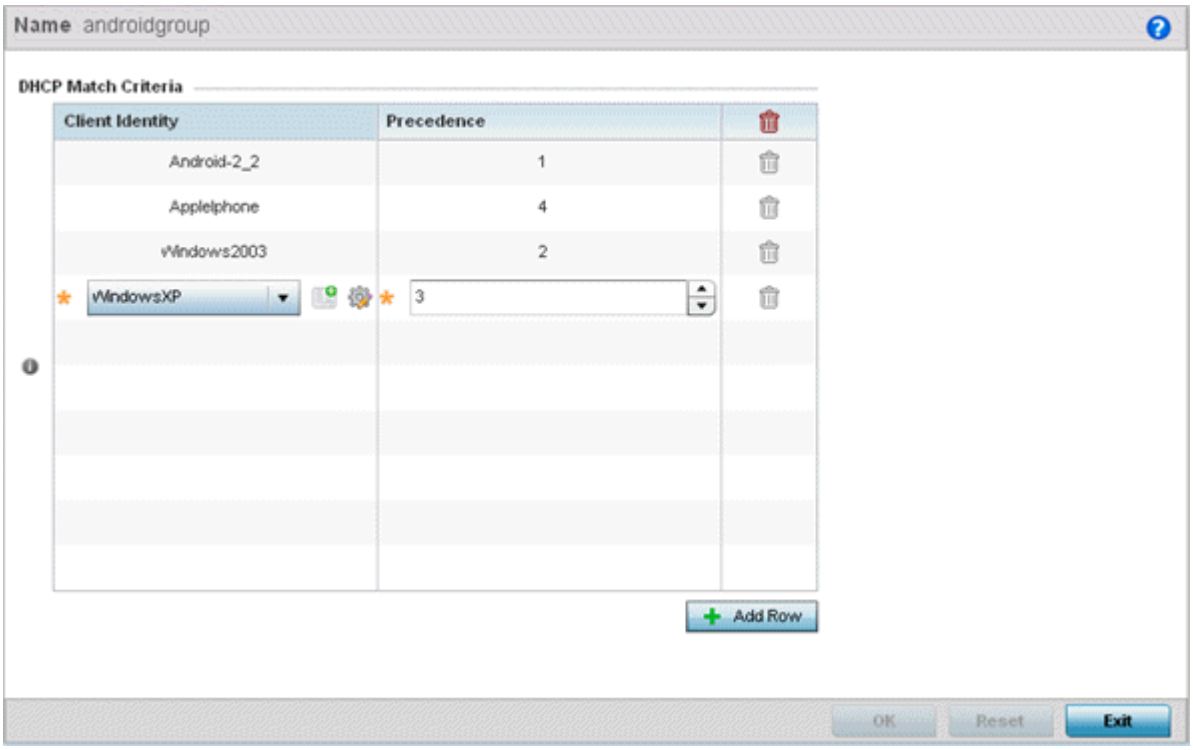



**Figure 364: Security - Device Fingerprinting - Client Identity Group - New Client Identity Group**

13 From the drop-down, select the **Client Identity Policy** to include in this group.

Use the buttons next to the drop-down to manage and create new Client Identity policies.

14 Use the **Precedence** control to set the precedence for the Client Identity.

This index sets the sequence the client identity in this Client Identity Group is checked or matched.

15 Click **OK** to save changes.

Click **Reset** to revert all changes made to this screen.

Click **Exit** to close the Client Identity Group screen.

## Configuring MAC Firewall Rules

Access points can use MAC based firewalls like Access Control Lists (ACLs) to filter and mark packets based on the IP from which they arrive, as opposed to filtering packets on Layer 2 ports.

Optionally, filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

Note
Once defined, a set of MAC firewall rules must be applied to an interface to be a functional filtering tool.

To add or edit a MAC based firewall rule policy:

1 Select **Configuration** > **Security** > **Wireless Firewall** > **MAC Firewall Rules** to display existing IP firewall rule policies.

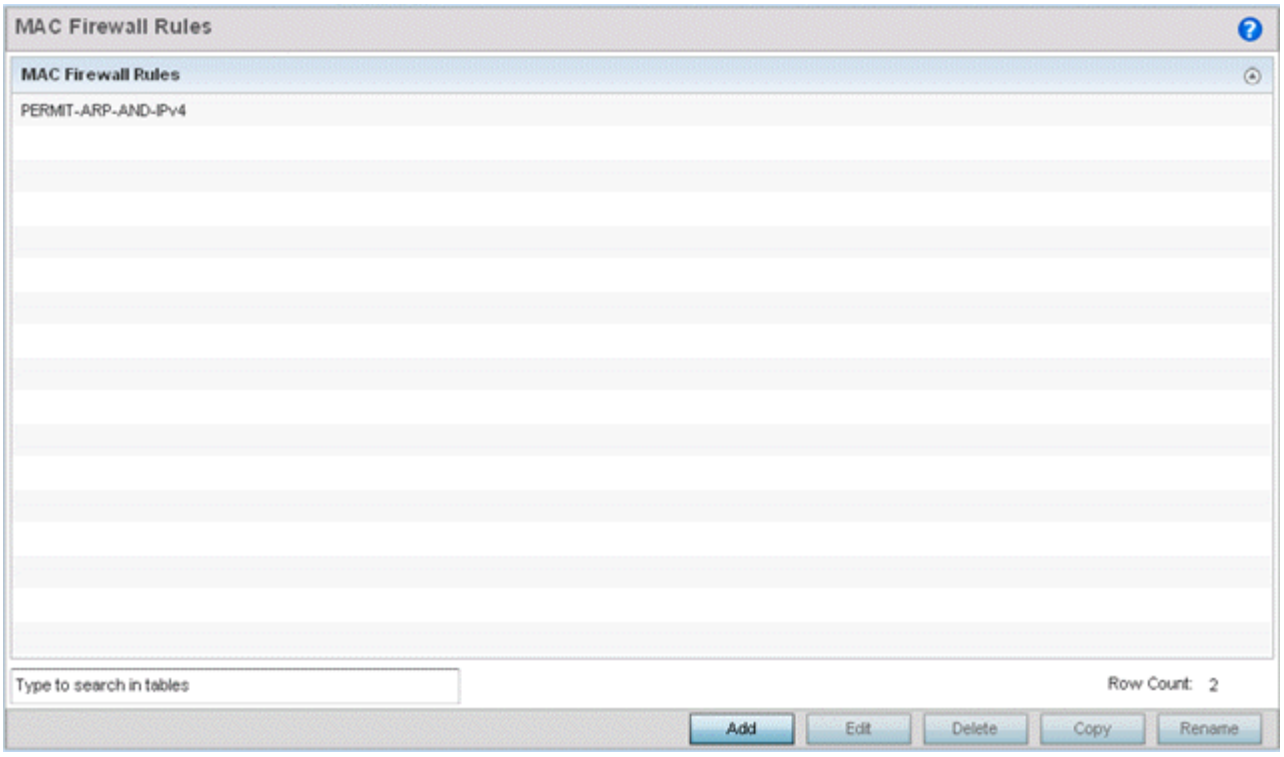



**Figure 365: MAC Firewall Rules Screen**

2 Select **Add** to create a new MAC firewall rule.

Select an existing policy and click **Edit** to modify the attributes of that rule's configuration.

3 Select the added row to expand it into configurable parameters for defining the MAC-based firewall rule.

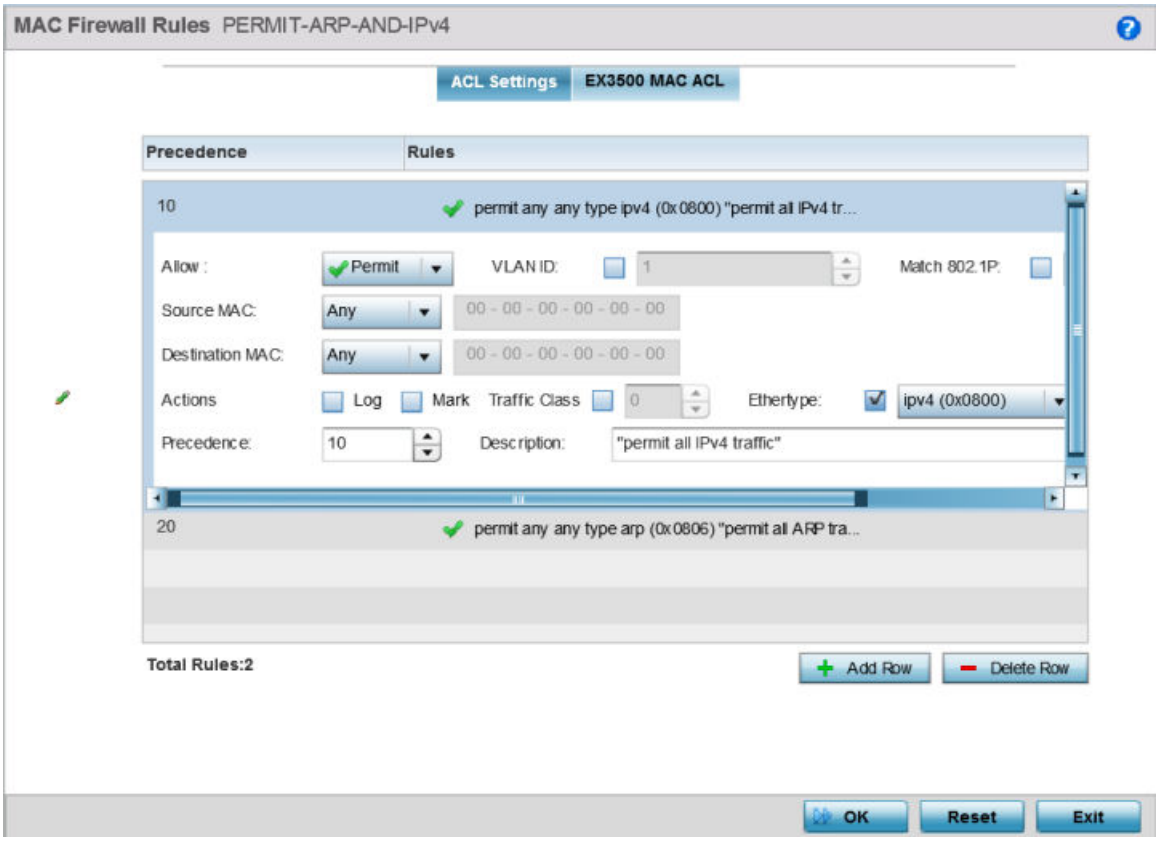



**Figure 366: MAC Firewall Rules Screen - Adding a New Rule**

4 If you are adding a new **MAC Firewall Rule**, provide a name up to 32 characters to help describe its filtering configuration.

5 Define the following parameters for the MAC firewall rule:

| | |
|---|---|
| Allow | Every MAC firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:<br>• Deny - Instructs the firewall to prevent a packet from proceeding to its destination.<br>• Permit - Instructs the firewall to allow a packet to proceed to its destination. |
| Source and Destination MAC | Enter both source and destination MAC addresses. Access points use the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask. |
| Action | The following actions are supported:<br>• Log - Events are logged for archive and analysis.<br>• Mark - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.<br>  • VLAN 802.1p priority.<br>  • DSCP bits in the IP header.<br>• Mark, Log - Conducts both mark and log functions. |

| | |
|---|---|
| Precedence | Use the spinner control to specify a precedence for this MAC firewall rule between 1 - 1500. Rules with lower precedence are always applied first to packets. |
| VLAN ID | Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). The VLAN ID can be from 1 - 4094. |
| Traffic Class | Select this option to enable filtering using Traffic Class. Use the spinner control to specify a traffic class. Traffic class can be from 1 - 10. |
| Match 802.1P | Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting between 0 - 7. |
| Ethertype | Use the drop-down menu to specify an Ethertype of either other, ipv4, arp, rarp, appletalk, aarp, mint, wisp,ipx, 802.1q and ipv6. An Ethertype is a twooctet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. |
| Description | Provide a description (up to 64 characters) for the rule to help differentiate it from others with similar configurations. |

6 Select **+ Add Row** as needed to add additional MAC firewall rule configurations.
Select the **- Delete Row** icon as required to remove selected MAC firewall rules.

7 Select **OK** when completed to update the MAC firewall rules.
Select **Reset** to revert to its last saved configuration.

## Wireless IPS (WIPS)

The access point supports *Wireless Intrusion Protection Systems* (WIPS) to provide continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. An access point supports WIPS through the use of dedicated sensor devices designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.

Unauthorized APs are untrusted and unsanctioned access points connected to a LAN that accept client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured access points that do not adhere to corporate policies. An attacker can install a unauthorized AP with the same ESSID as the authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a man-in-the middle attack or take control of wireless clients to launch denial-of-service attacks.

Note
WIPS is not supported natively by an AP6521 model access point and must be deployed using an external WIPS server resource.

A WIPS server can be deployed as a dedicated solution within a separate enclosure. When used with associated access point radios, a WIPS deployment provides the following enterprise class security management features:

- *Threat Detection* - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the wireless network.
- *Rogue Detection and Segregation* - A WIPS supported network distinguishes itself by both identifying and categorizing nearby access points. WIPS identifies threatening versus non-

threatening access points by segregating access points attached to the network (unauthorized APs) from those not attached to the network (neighboring access points). The correct classification of potential threats is critical for administrators to act promptly against rogues and not invest in a manual search of thousands of neighboring access points.

- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues though the identification and removal of their connected access points.
- *WEP Cloaking* - WEP Cloaking protects organizations using the Wired Equivalent Privacy (WEP) security standard to protect networks from common attempts used to crack encryption keys.

To define an access point's WIPS configuration:

1 Select the Configuration tab from the Web user interface. 2 3

2 Select **Security**.

3 Select **Wireless IPS** to display existing Wireless Intrusion Protection policies.

The Wireless IPS screen displays the Settings tab by default.

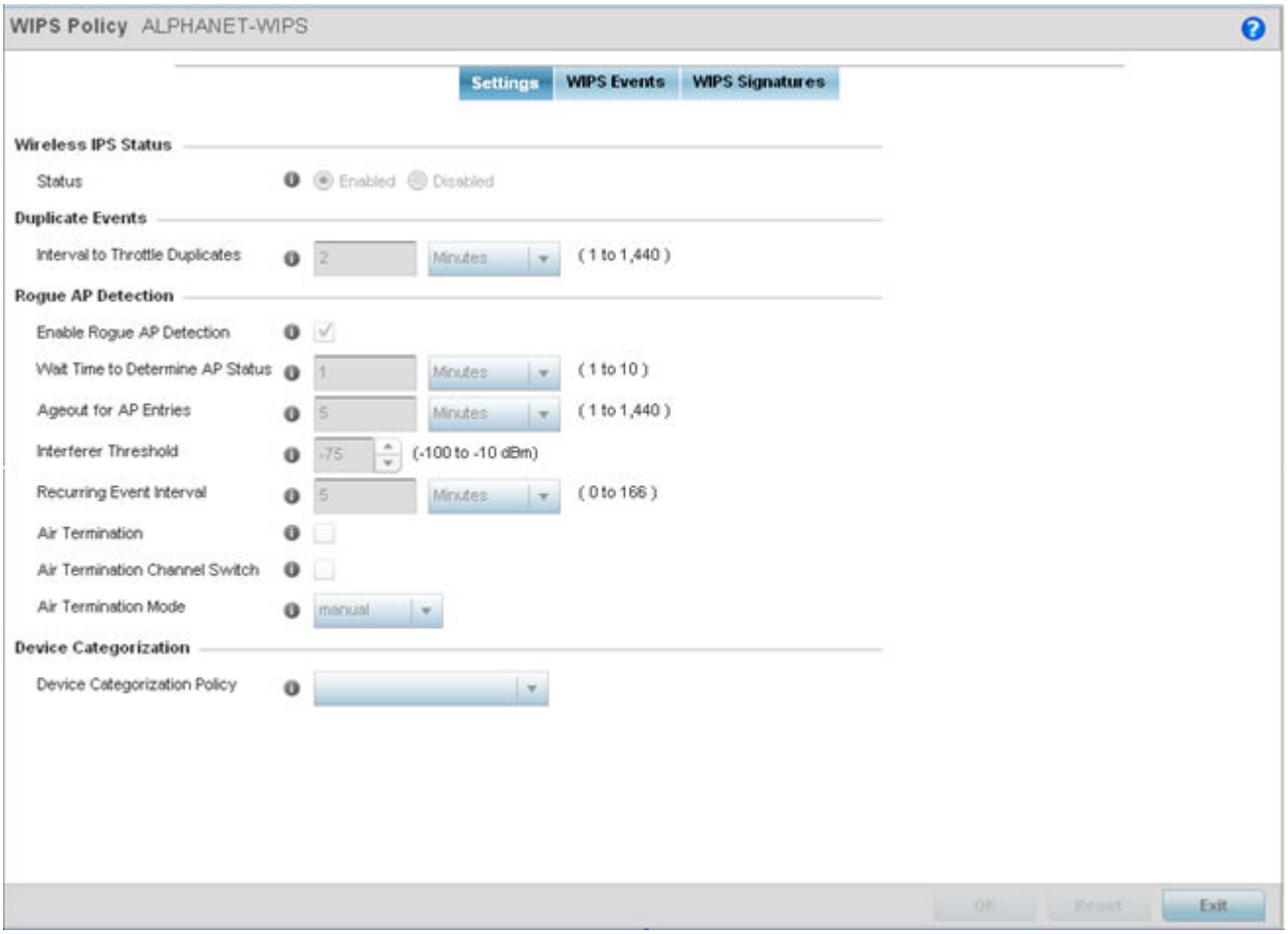



**Figure 367: Wireless IPS Screen - Settings Tab**

4 Select the **Activate Wireless IPS Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration.

Ensure that this option stays selected to apply the configuration to the access point profile.

5 In the **Wireless IPS Status** field, select either **Enabled** or **Disabled** to activate or deactivate WIPS.

The default setting is **Enabled**.

6 Enter an **Interval to Throttle Duplicates** in either Seconds (1 - 86,400), Minutes (1 - 1,400), Hours (1 - 24) or Days (1).

This interval represents the duration event duplicates are not stored in history. The default setting is 120 seconds.

7 Refer to the **Rogue AP Detection** field to define the following detection settings for this WIPS policy:

| | |
|---|---|
| Enable Rogue AP Detection | Select the check box to enable the detection of unsanctioned APs from this WIPS policy. The default setting is disabled. |
| Wait Time to Determine AP Status | Define a wait time in either Seconds (10 - 600) or Minutes (0 - 10) before a detected AP is interpreted as a rogue (unsanctioned) device, and potentially removed. The default interval is 1 minute. |
| Ageout for AP Entries | Set the interval the WIPS policy uses to ageout rogue devices. Set the policy in either Seconds (30 - 86,400), Minutes (0- 1,440), Hours (1 - 24) or Days (1). The default setting is 5 minutes. |
| Interferer Threshold | Specify a RSSI threshold (from -100 to -10 dBm) after which a detected access point is classified as an interferer (rogue device). |
| Recurring Event Interval | Set an interval that, when exceeded, duplicates a rogue AP event if the rogue devices is still active (detected) in the network. The default setting is 5 minutes. |
| Air Termination | Select this option to enable the termination of detected rogue AP devices. Air termination lets you terminate the connection between your wireless LAN and any access point or client associated with it. If the device is an access point, all clients dis-associated with the access point. If the device is a client, its connection with the access point is terminated. This setting is disabled by default. |
| Air Termination Channel Switch | Select this option to allow neighboring access point to switch channels for rogue AP termination. This setting is disabled by default. |
| Air Termination Mode | If termination is enabled, use the drop-down menu to specify the termination mode used on detected rogue devices. The default setting is manual. |

8 Refer to the **Device Categorization** field to associate a Device Categorization Policy with this Wireless IPS policy.

Select the **Add** icon to create a new Device Categorization policy, or select the **Edit** icon to modify an existing Device Categorization policy. For more information on Device Categorization, see Device Categorization on page 781.

9 Select **OK** to update the settings.

Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.

10 Select the WIPS Events tab.

Ensure that the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters. This option needs to remain selected to apply the WIPS configuration to the access point profile.

The Excessive tab displays by default, with additional MU Anomaly and AP Anomaly tabs also available.

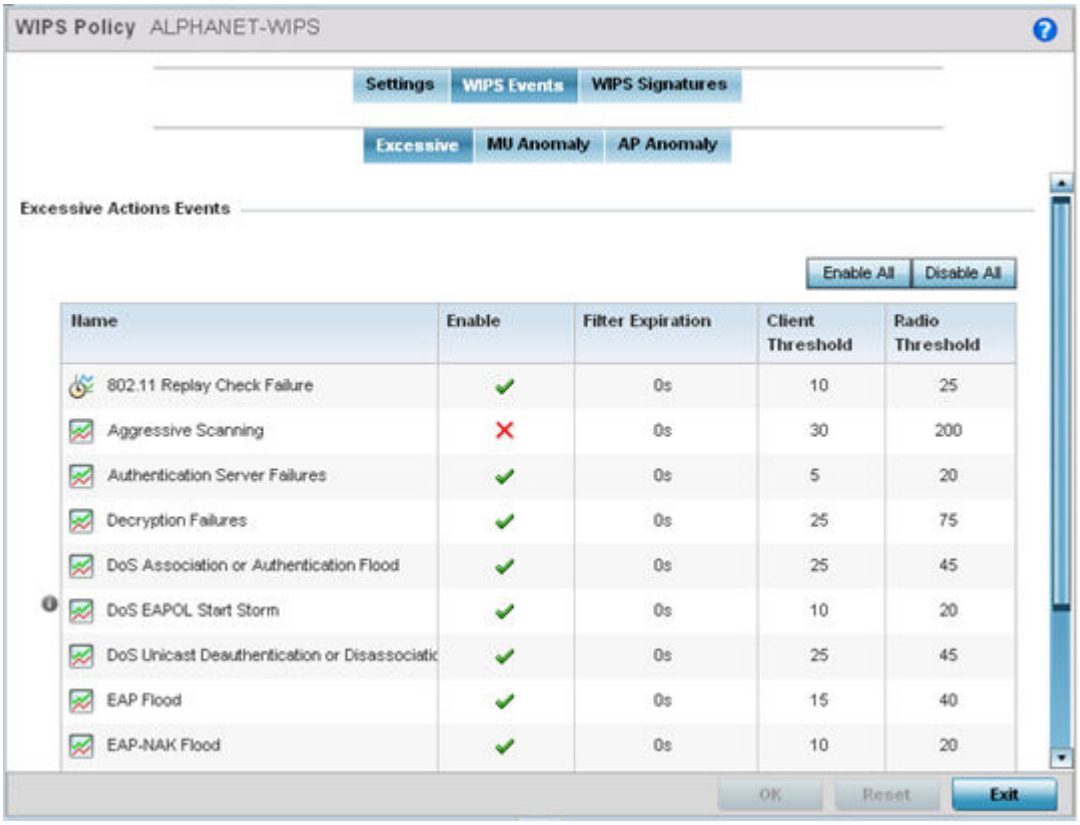



**Figure 368: Wireless IPS Screen - WIPS Events - Excessive Tab**

The Excessive tab lists events with the potential of impacting network performance. An administrator can enable or disable event filtering and set the thresholds for the generation of the event notification and filtering action.

An Excessive Action Event is an event where an action is performed repetitively and continuously. DoS attacks come under this category. Use the **Excessive Actions Events** table to select and configure the action taken when events are triggered.

11 Set the following **Excessive Action Event** configurations:

| | |
|---|---|
| Name | Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted. |
| Enable | Displays whether tracking is enabled for each event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default. |

| | |
|---|---|
| Filter Expiration | Set the duration an event generating client is filtered. This creates a special ACL entry, and frames coming from the client are dropped. The default setting is 0 seconds. This value is applicable across the RF Domain. If a station is detected performing an attack and is filtered by an access point, the information is passed to the domain controller. The domain controller then propagates this information to all the access points in the RF Domain. |
| Client Threshold | Set the client threshold after which the filter is triggered and an event generated. |
| Radio Threshold | Set the radio threshold after which an event is recorded to the event history. |

Use the **Enable All** button to enable all Excessive Action Events. Use **Disable All** to disable all Excessive Action Events.

12 Select **OK** to save the updates to the to Excessive Actions configuration used by the WIPS policy.

Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper left-hand side of the access point user interface.

13 Select the MU Anomaly tab.

Ensure that the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

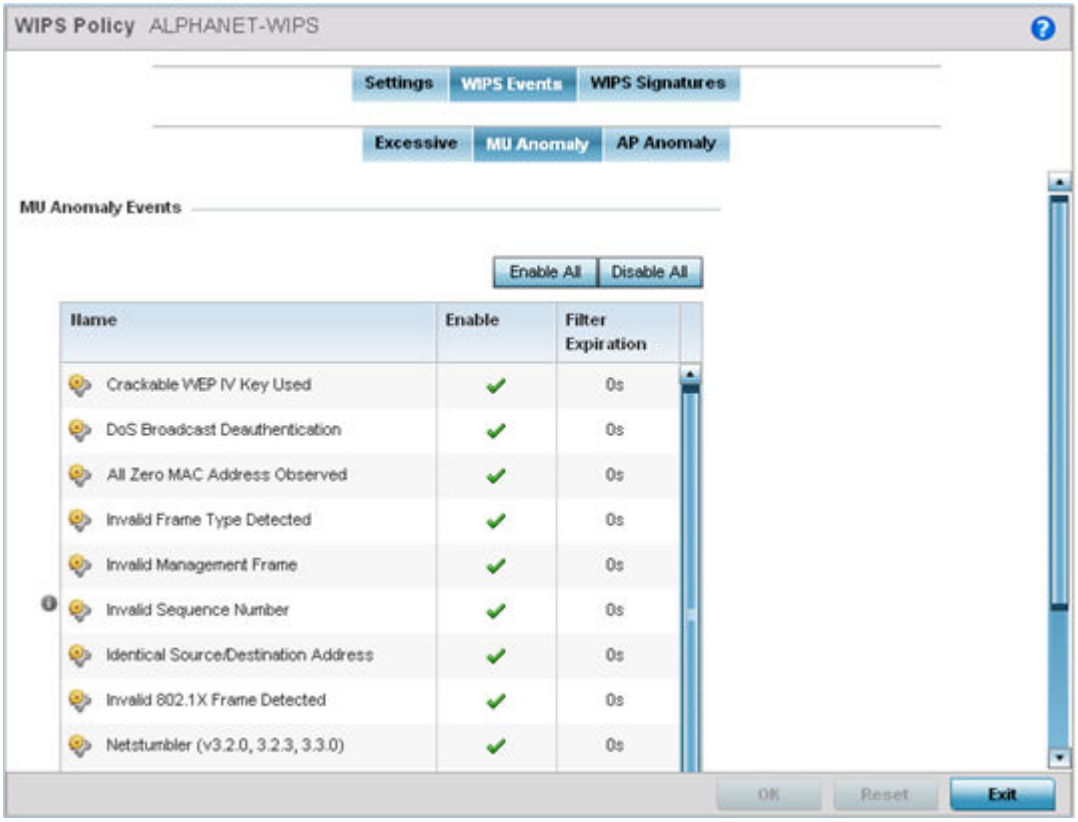



**Figure 369: Wireless IPS Screen - WIPS Events - MU Anomaly Tab**

**MU Anomaly** events are suspicious events by wireless clients that can compromise the security and stability of the network. Use the MU Anomaly screen to set the intervals clients can be filtered upon the generation of each event.

14 Set the following **MU Anomaly Event** configurations:

| | |
|---|---|
| Name | Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted. |
| Enable | Displays whether tracking is enabled for each MU Anomaly event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold. A red “X” defines the event as disabled, and not tracked by the WIPS policy. Each event is disabled by default. |
| Filter Expiration | Set the duration a client is filtered. This creates a special ACL entry, and frames coming from the client are silently dropped. The default setting is 0 seconds. For each violation, define a time to filter value (in seconds) which determines how long received packets are ignored from an attacking device once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed. |

Use the **Enable All** button to enable all MU Anomaly rules. Use **Disable All** to disable all MU Anomaly rules.

15 Select **OK** to save the updates to the MU Anomaly configuration used by the WIPS policy.

Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper left-hand side of the access point user interface.

16 Select the AP Anomaly tab.

Ensure that the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

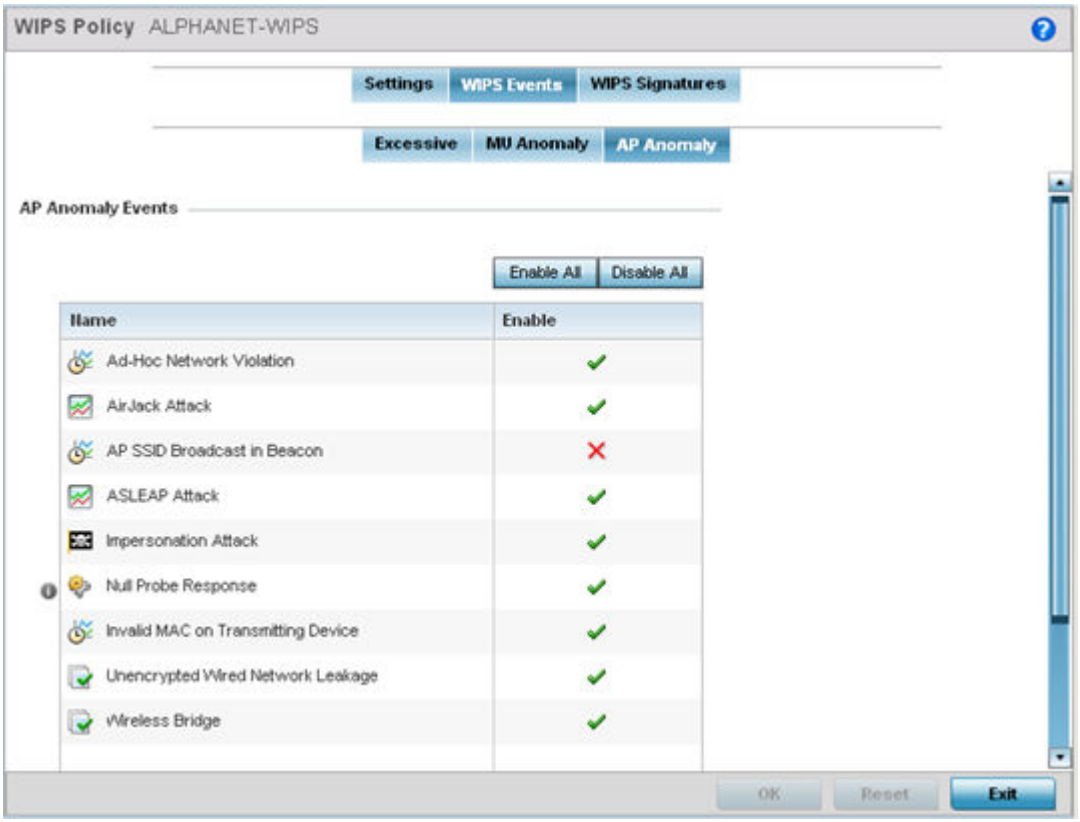



**Figure 370: Wireless IPS Screen - WIPS Events - AP Anomaly Tab**

**AP Anomaly** events are suspicious frames sent by neighboring APs. Use the AP Anomaly tab to enable or disable an event.

17 Enable or disable the following **AP Anomaly Events**:

| | |
|---|---|
| Name | Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted. |
| Enable | Displays whether tracking is enabled for each AP Anomaly event. Use the drop-down menu to enable/disable events as required. A green check mark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default. |

Use the **Enable All** button to enable all AP Anomaly events. Use **Disable All** to disable all AP Anomaly events.

18 Select **OK** to save the updates to the AP Anomaly configuration used by the WIPS policy.

Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper left-hand side of the access point user interface.

19 Select the WIPS Signatures tab.

Ensure that the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

A WIPS signature is the set or parameters, or pattern, used by WIPS to identify and categorize particular sets of attack behaviors in order to classify them.

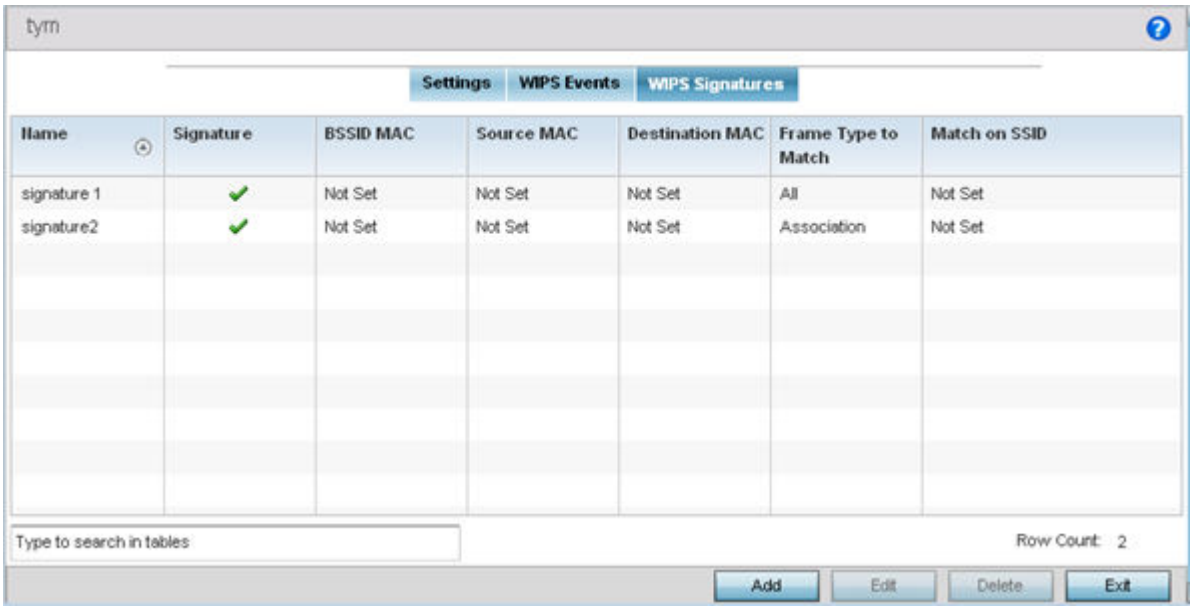



**Figure 371: Wireless IPS Screen - WIPS Signatures Tab**

20 The WIPS Signatures tab displays the following read-only configuration data:

| | |
|---|---|
| Name | Lists the name assigned to each signature when it was created. A signature name cannot be modified as part of the edit process. |
| Signature | Displays whether the signature is enabled. A green checkmark defines the signature as enabled. A red "X" defines the signature as disabled. Each signature is disabled by default. |
| BSSID MAC | Displays each BSS ID MAC address used for matching purposes. |
| Source MAC | Displays each source packet MAC address for matching purposes. |
| Destination MAC | Displays each destination packet MAC address for matching purposes. |
| Frame Type to Match | Lists the frame types specified for matching with the WIPS signature. |
| Match on SSID | Lists each SSID used for matching purposes. |

21 Select **Add** to create a new WIPS signature, **Edit** to modify the attributes of a selected WIPS signature, or **Delete** to remove obsolete signatures from the list of those available.

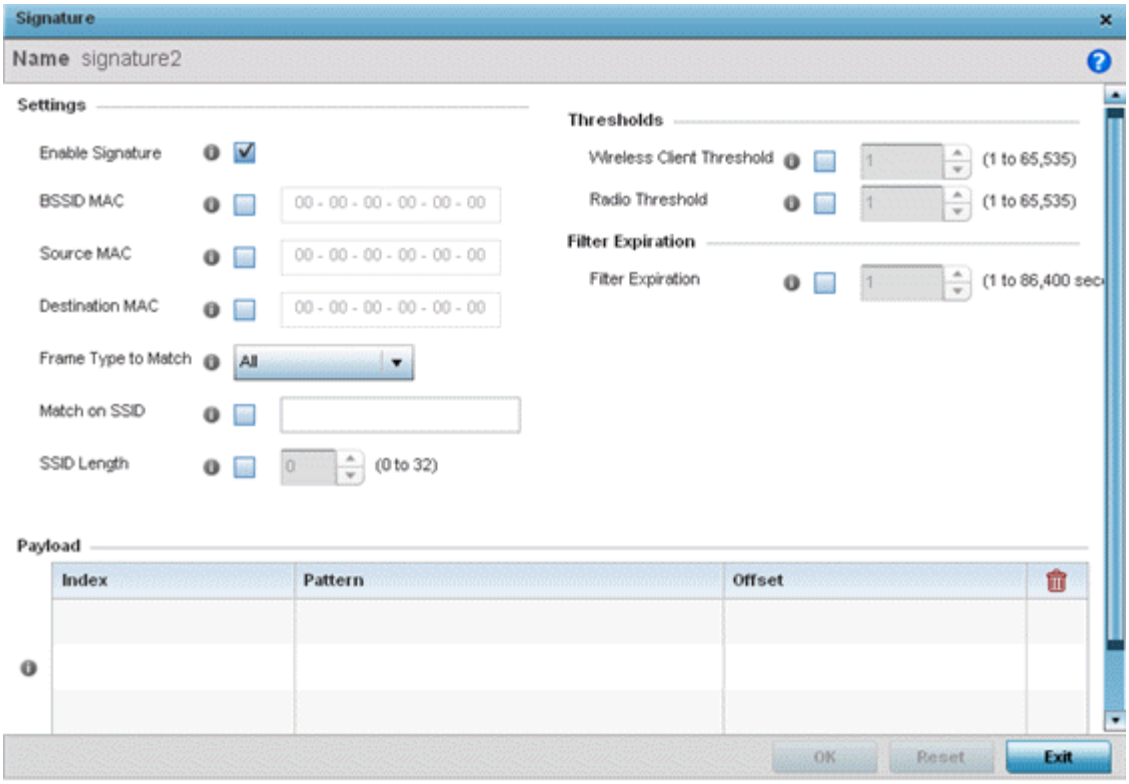



**Figure 372: Wireless Signature Configuration Screen**

22 If you are adding a new WIPS signature, define a **Name** to distinguish it from others with similar configurations.

The name cannot exceed 64 characters.

23 Set the following network address information for a new or modified WIPS Signature:

| | |
|---|---|
| Enable Signature | Select the radio button to enable the WIPS signature for use with the profile. The default signature is enabled. |
| BSSID MAC | Define a BSS ID MAC address used for matching and filtering with the signature. |
| Source MAC | Define a source MAC address for the packet examined for matching, filtering and potential device exclusion using the signature. |
| Destination MAC | Set a destination MAC address for a packet examined for matching, filtering and potential device exclusion using the signature. |
| Frame Type to Match | Use the drop-down menu to select a frame type for matching with the WIPS signature. |
| Match on SSID | Sets the SSID used for matching. Ensure it is specified properly or the SSID won't be properly filtered. |
| SSID Length | Set the character length of the SSID used for matching purposes. The maximum length is 32 characters. |

24 Refer to the **Thresholds** field to set the thresholds used as filtering criteria.

| | |
|---|---|
| Wireless Client Threshold | Specify the threshold limit per client that, when exceeded, signals the event. The configurable range is from 1 - 65,535. |
| Radio Threshold | Specify the threshold limit per radio that, when exceeded, signals the event. The configurable range is from 1 - 65,535. |

25 Set a **Filter Expiration** from 1 - 86,400 seconds that specifies the duration a client is excluded from radio association when responsible for triggering a WIPS event.

26 Refer to the **Payload** table to set a numerical index and offset for the WIPS signature.

27 Select **OK** to save the updates to the WIPS Signature configuration.

Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked and applied to the access point profile by selecting **Activate Wireless IPS Policy** from the upper left-hand side of the access point user interface.

## Device Categorization

A proper classification and categorization of access points and clients can help suppress unnecessary unauthorized access point alarms, and allow an administrator to focus on alarms on devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization.

Authorized access points and clients are generally known to you and conform with your organization's security policies. Unauthorized devices are those detected as interoperating within the network, but have not been approved. These devices should be filtered to avoid jeopardizing the data managed by the access point and its connected clients. Use the Device Categorization screen to apply neighboring and sanctioned (approved) filters on peer access points operating in this access point's radio coverage area. Detected client MAC addresses can also be filtered based on their classification in this access point's coverage area.

To categorize access points and clients as authorized or unauthorized:

1 Select **Configuration** > **Security** > **Device Configuration** to display existing device categorization policies.

The Device Categorization screen lists the device authorizations defined thus far.

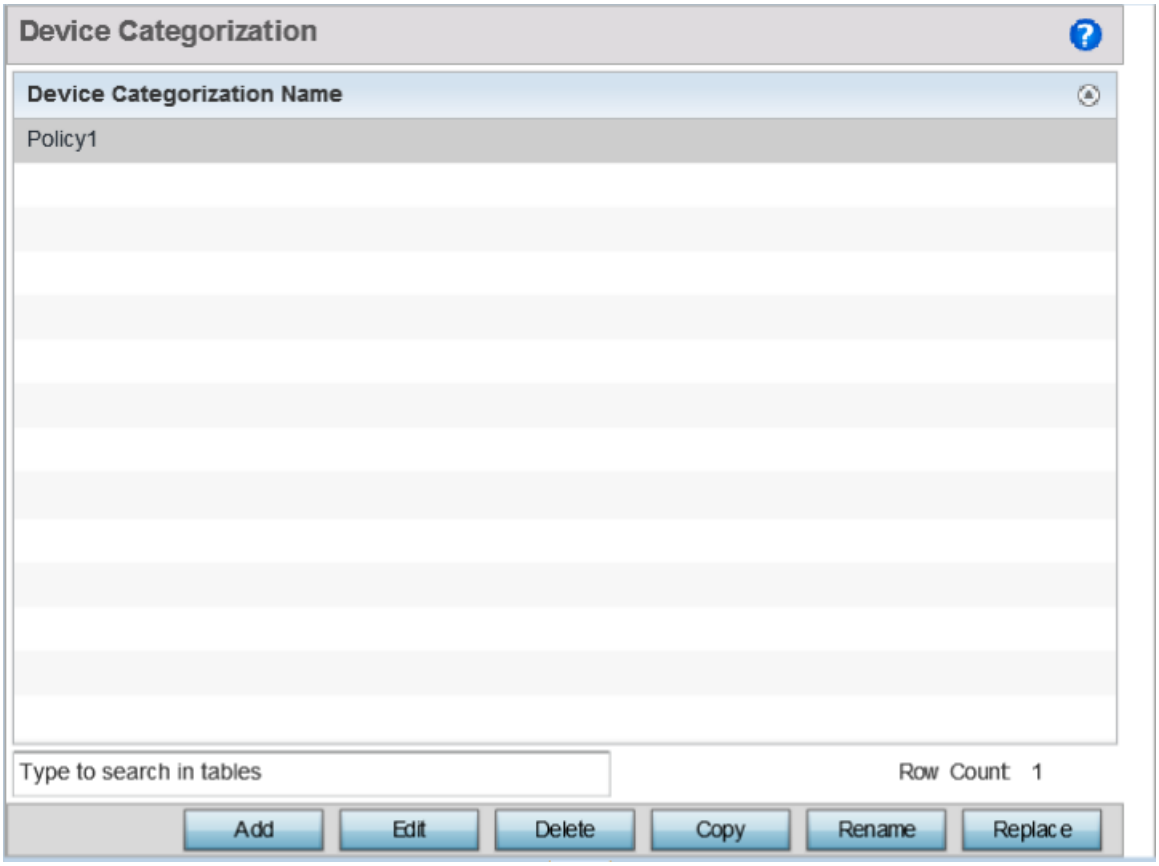



**Figure 373: Device Categorization screen**

2 Select **Add** to create a new Device Categorization policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

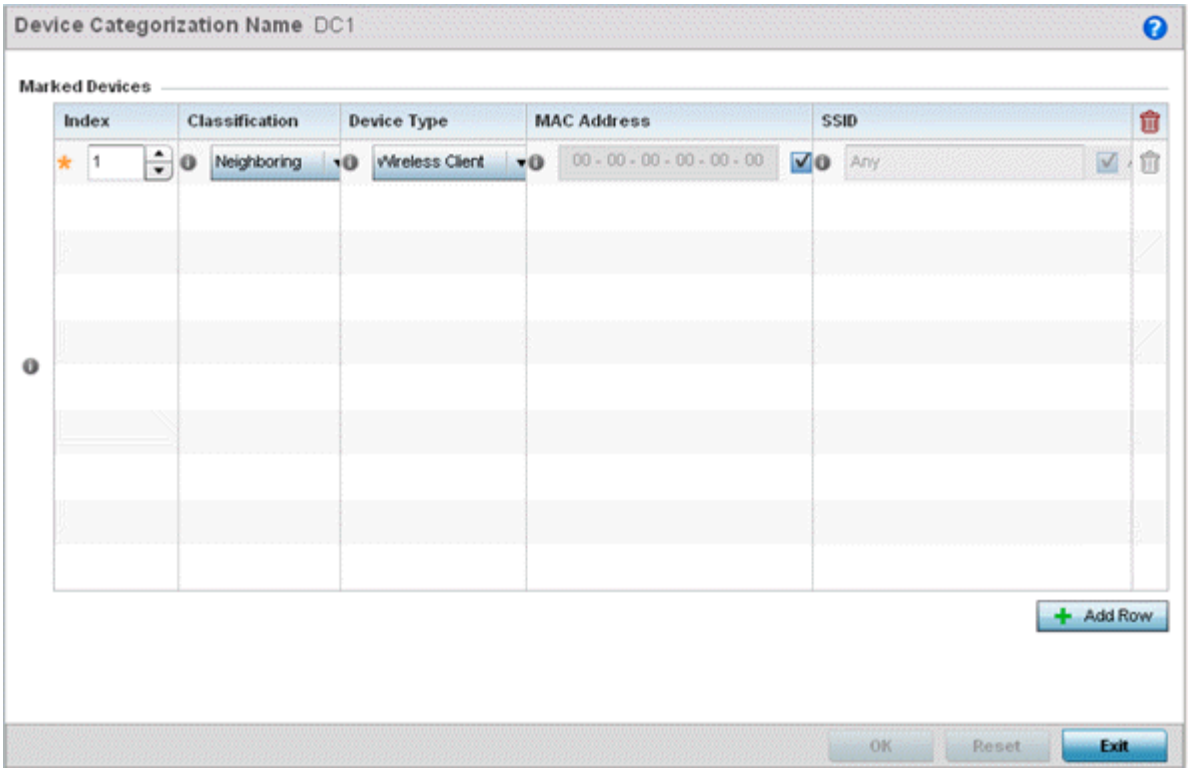



**Figure 374: Device Categorization Screen - Marked Devices**

3 If you are creating a new Device Categorization filter, give it a **Name** (up to 32 characters).

Select **OK** to save the name and enable the remaining device categorization parameters.

4 Select **+ Add Row** to populate the **Marked Devices** field with parameters for classifying an access point or client and defining the target device's MAC address and SSID.

Select the red **(-) Delete Row** icon as needed to remove an individual table entry.

5 Refer to Thresholds field to set the thresholds used as filtering criteria.

| | |
|---|---|
| Index | Use the spinner control to designate a index value to this entry. Use a value in the range 1 - 1000. |
| Classification | Use the drop-down menu to designate the target device as either **`Sanctioned`** or **`Neighboring`**. |
| Device Type | Use the drop-down menu to designate the target device as either an access point or client. |
| MAC Address | Enter the factory coded MAC address of the target device. This address is hard coded by the device manufacturer and cannot be modified. This MAC address is defined as authorized or unauthorized as part of the device categorization process. |
| SSID | Enter the SSID of the target device requiring categorization. The SSID cannot exceed 32 characters. |

6 Select **OK** to save the updates to the **Marked Devices** list.

Select **Reset** to revert to the last saved configuration.

## Security Deployment Considerations

Before defining a firewall supported configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Firewalls implement access control policies. So if you do not have an idea of what kind of access to allow or deny, a firewall is of little value.
- It's important to recognize the firewall's configuration is a mechanism for enforcing a network access policy.
- A role based firewall requires an advanced security license to apply inbound and outbound firewall policies to users and devices. Role based firewalls are not supported on AP6521 model access point.
- Firewalls cannot protect against tunneling over application protocols to poorly secured wireless clients.
- Firewalls should be deployed on WLANs implementing weak encryption to minimize access to trusted networks and hosts in the event the WLAN is compromised.
- Firewalls should be enabled when providing Captive Portal guest access. Firewalls should be applied to Captive Portal enabled WLANs to prevent guest user traffic from being routed to trusted networks and hosts.
- Before configuring WIPS support, refer to the following deployment guidelines to ensure the configuration is optimally effective:
- WIPS is best utilized when deployed in conjunction with a corporate or enterprise wireless security policy. Since an organization's security goals vary, the security policy should document site specific concerns. The WIPS system can then be modified to support and enforce these additional security policies
- WIPS reporting tools can minimize dedicated administration time. Vulnerability and activity reports should automatically run and be distributed to the appropriate administrators. These reports should highlight areas to be to investigated and minimize the need for network monitoring.
- It is important to keep your WIPS system firmware and software up to date. A quarterly system audit can ensure firmware and software versions are current.
- Only a trained wireless network administrator can determine the criteria used to authorize or ignore devices. You may want to consider your organization's overall security policy and your tolerance for risk versus users' need for network access. Some questions that may be useful in deciding how to classify a device are:
- Does the device conform to any vendor requirements you have?
- What is the signal strength of the device? Is it likely the device is outside your physical radio coverage area?
- Is the detected access point properly configured according to your organization's security policies?
- Trusted and known access points should be added to an sanctioned AP list. This will minimize the number of unsanctioned AP alarms received.

# 10 Services Configuration



The WING software supports services providing captive portal access, leased DHCP IP address assignments to requesting clients, and local RADIUS client authentication.

For more information, refer to the following:

- Captive Portal Policies on page 785
- Setting the DNS Whitelist Configuration on page 799
- Setting the DHCP Configuration on page 800
- Setting the Bonjour Gateway Configuration on page 814
- Setting the DHCPv6 Server Policy on page 818
- Setting the RADIUS Configuration on page 824
- Setting the Imagotag Policy on page 845
- Setting the URL List on page 843

Refer to Services Deployment Considerations on page 848 for tips on how to optimize the access point's configuration.

## Captive Portal Policies

A *captive portal* is an access policy for providing guests temporary and restrictive access to the controller or service platform managed network.

A captive portal policy provides secure authenticated controller or service platform access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional Terms and Agreement, Welcome, Fail and No Service pages provide the administrator with a number of options on captive portal screen flow and user appearance.

Captive portal authentication is used primarily for guest or visitor access, but is increasingly used to provide authenticated access to private network resources when 802.1X EAP is not a viable option.

Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Authentication for captive portal access requests is performed using a username and password pair, authenticated by an integrated RADIUS server. Authentication for private network access is conducted either locally on the requesting wireless client, or centrally at a datacenter.

Captive portal uses a Web provisioning tool to create guest user accounts directly on the controller or service platform. The connection medium defined for the Web connection is either HTTP or HTTPS. Both HTTP and HTTPS use a request and response procedure clients follow to disseminate information to and from requesting wireless clients.

To access the captive portal configuration screen:

1 Go to **Configuration → Services**.

The Captive Portal main screen displays. Review existing captive portal configuration to determine if a new configuration warrants creation, an existing configuration warrants edition, or an existing configuration warrants deletion.

2 To add a new captive portal policy, click **Add**.

3 To edit or delete and existing captive portal policy, select the policy from those listed on the screen and click **Edit** or **Delete** as reuqired.

Refer to the following sections for configuring Captive Portal Policy parameters:

- Captive Portal Policy Basic Configuration on page 787
- Setting the DNS Whitelist Configuration on page 799
- Captive Portal Deployment Considerations

## Captive Portal Policy Basic Configuration

1 Select **Add** to create a new captive portal policy, **Edit** to modify an existing policy, or **Delete** to remove an existing captive portal policy.

Select **Copy** to create a copy of an existing captive portal policy and use it for further customization. Select **Rename** to change the name of an existing policy or copy a policy to a different location.

Select **Replace** to replace an existing captive portal policy with another captive portal policy.

A Basic Configuration screen displays by default. Define the policy's security, access, and whitelist basic configuration before actual HTML pages can be defined for guest user access requests.

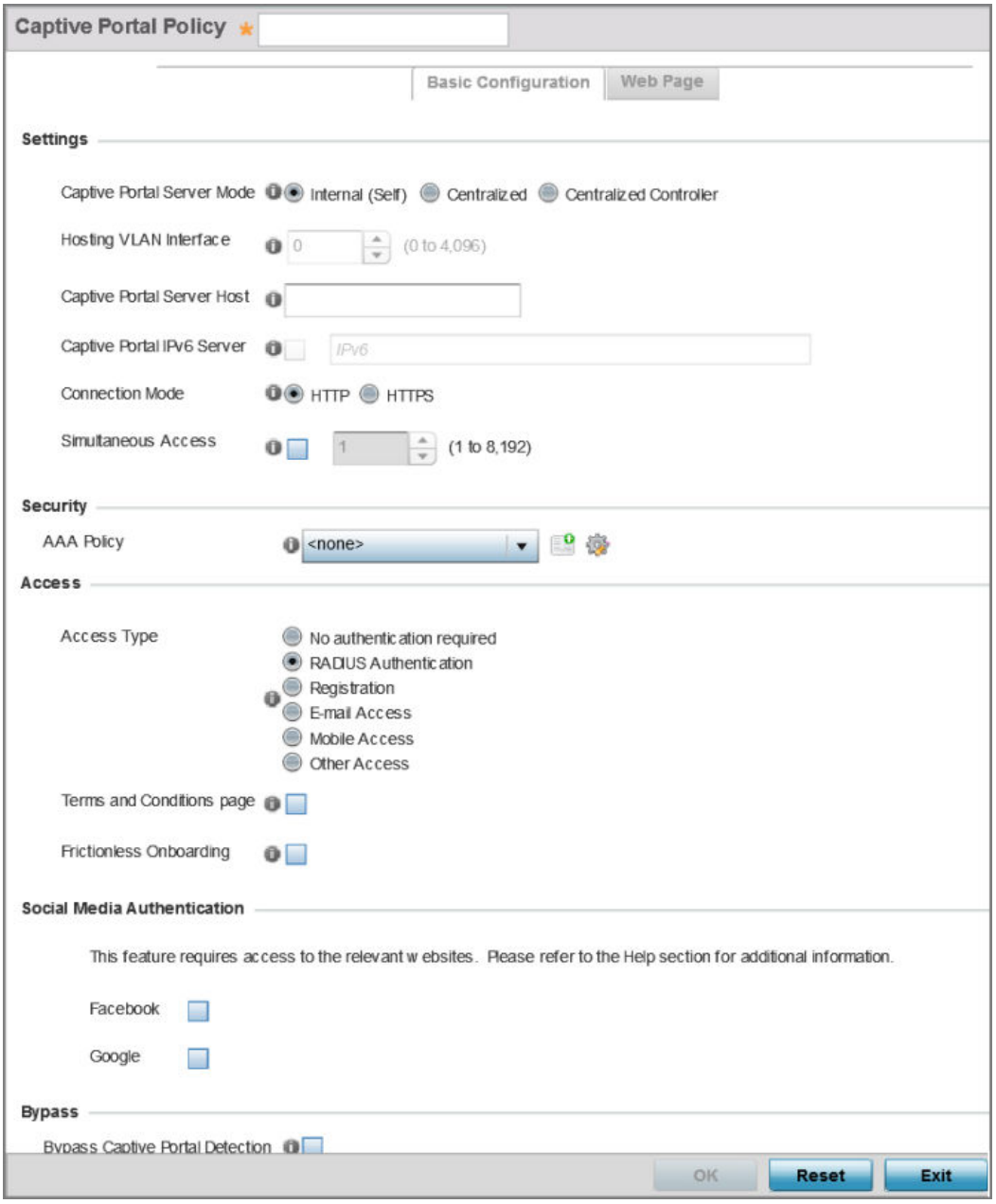



**Figure 375: Captive Portal Policy - Add/Edit - Basic Configuration Tab**

2 Define the following captive portal policy Settings:

| | |
|---|---|
| Captive Portal Policy | If you are creating a new policy, assign a name representative of its access permissions, location or intended wireless client user base. If you are editing an existing captive portal policy, the policy name cannot be modified. The name cannot exceed 32 characters. |
| Captive Portal Server Mode | Set the mode as either **`Internal (Self)`**, **`Centralized`** or **`Centralized Controller`**. Select the Internal (Self) radio button to maintain the captive portal configuration (Web pages) internally. Select the Centralized radio button if the captive portal is supported on an external server. Select the Centralized Controller radio button if the captive portal is supported on a centralized controller or service platform. The default value is Internal (Self). |
| Hosting VLAN Interface | When **`Centralized`** is selected as the **Captive Portal Server Mode**, specify the VLAN (between 0 and 4096) for client communication. Select 0 to use the default client VLAN. 0 is the default setting. |
| Captive Portal Server Host | When **`Centralized`** is selected as the **Captive Portal Server Mode**, set a numeric IP address (or DNS hostname) for the server validating guest user permissions for the captive portal policy.<br>When **`Centralized Controller`** is selected, use this field to provide the hostname of the controller or controllers acting as the captive portal server host. |
| Captive Portal IPv6 Server | Set a numeric IP address (non DNS hostname) for the server validating guest user permissions for the captive portal policy. This option is available only if you are hosting the captive portal on an external (**`Centralized`**) server resource. |
| Connection Mode | Select either **`HTTP`** or **`HTTPS`** to define the connection medium to the Web server. We recommend the use of HTTPS because it affords some additional data protection HTTP cannot provide. The default value, however, is HTTP. |
| Simultaneous Access | Select this check box and use the spinner control to set from 1-8192 users (client MAC addresses) allowed simultaneous access to the captive portal and its resources. |

3 Use the **AAA Policy** drop-down menu to select the *Authentication, Authorization and Accounting* (AAA) policy used to validate user credentials and provide captive portal access to the network.

If no AAA policies exist, one must be created by selecting the **Create** icon, or an existing AAA policy can be selected and modified by selected it from the drop-down menu and selecting the **Edit** icon.

For information on creating a AAA policy, see AAA Policy on page 688.

4 Set the following **Access** parameters to define captive portal access, RADIUS lookup information, and whether the Login pages contain agreement terms that must be accepted before access is granted to controller or service platform resources using the captive portal:

| | |
|---|---|
| Access Type | Select the authentication scheme applied to clients requesting captive portal guest access to the WiNG network. Within the WiNG UI there are six options. The WiNG CLI uses five options. User interface options include:<br>• **No authentication required** - Requesting clients are redirected to the captive portal Welcome page without authentication.<br>• **RADIUS Authentication** - A requesting client's user credentials require authentication before access to the captive portal is permitted. This is the default setting.<br>• **Registration** - A requesting client's user credentials require authentication through social media credential exchange.<br>• **Email Access** - Clients use E-mail username and passwords for authenticating their captive portal session. Optionally set whether E-mail access requests are RADIUS validated.<br>• **Mobile Access** - Mobile clients use their device's access permissions for authenticating their captive portal session. Optionally set whether mobile access requests are RADIUS validated.<br>• **Other Access** - Requesting guest clients use a different means of captive portal session access (aside from E-mail or mobile device permissions). Optionally set whether these other access requests are RADIUS validated. |
| Terms and Conditions page | Select this option (with any access type) to include terms that must be adhered to for clients requesting captive portal access. These terms are included in the Terms and Conditions page when **`No authentication required`** is selected as the access type, otherwise the terms appear in the Login page. The default setting is disabled. |
| Frictionless Onboarding | Select this option to enable wireless clients, associated with guest WLANs, to self-register with the ExtremeGuest server. In other words, this feature enables frictionless on-boarding of guest users to the ExtremeGuest server.<br>It also provides an integration API, as a means of on-boarding guest users through a loyalty application.<br>In the captive portal, set access-type as 'Registration', enable 'Frictionless Onboarding', and provide the Localization URL to trigger a one-time redirect on demand. The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.<br><br>Note: If enabling this feature, in the WLAN (using this captive-portal) set the following parameters: authentication-type as 'MAC' and registration-mode as 'device'. Enable the 'External Controller' and 'Follow AAA' options. Use the AAA Policy drop-down menu to specify the AAA policy. In the AAA policy, ensure that the authentication server configuration points to the ExtremeGuest server. |

5 Set the following **Social Media Authentication** parameters to utilize a requesting client's social media profile for captive portal registration:

| | |
|---|---|
| Facebook | If selected, the requesting client's guest user Facebook social media profile (collected from the social media server) is registered on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication. This option is disabled by default. |
| Google | If selected, the requesting client's guest user Google social media profile (collected from the social media server) is registered on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication. This option is disabled by default. |

6 Refer to the **Bypass** field to enable or disable Bypass Captive Portal Detection capabilities.

If enabled, captive portal detection requests are bypassed. This feature is disabled by default.

7 Set the following **Client Settings** to define client VLAN assignments, how long clients are allowed captive portal access, and when clients are timed out due to inactivity:

| | |
|---|---|
| RADIUS VLAN Assignment | Select this option to enable the RADIUS server to assign a VLAN post authentication. Once a captive portal user is authenticated, the user is assigned the VLAN as configured in the **Post Authentication VLAN** field. |
| Post Authentication VLAN | When this option is selected, a specific VLAN is assigned to the client upon successful authentication. The available range is from 1 - 4,096. |
| Client Access Time | Use the spinner control to define the duration wireless clients are allowed access to using the captive portal policy when there is no session time value defined for the RADIUS response. Set an interval from 10 - 10,800 minutes. The default interval is 1,440 minutes. |
| Inactivity Timeout | Use the drop-down menu to specify an interval in either minutes (1 - 1,440) or seconds (60 - 86,400) that, when exceeded, times out the session. The default is 10 minutes. |

8 Define the following **Loyalty App** settings to allow administrators to detect and report a captive portal client's usage of a selected (preferred) loyalty application:

| | |
|---|---|
| Enable | Select this option to report a captive portal client's loyalty application presence and store this information in the captive portal's user database. The client's loyalty application detection occurs on the Access Point to which the client is associated and allows a retail administrator to assess whether a captive portal client is using specific retail (loyalty) applications in their captive portal. This setting is enabled by default. |
| App Name | Use the drop-down menu to select an existing application to track for loyalty utilization by captive portal clients. This enables an administrator to assess whether patrons are accessing an application as expected in specific retail environments. To create an application if none exists suiting the specific reporting needs of captive portal clients, see Application on page 718. |

9 Use the **DNS Whitelist** parameter to create a set of allowed destination IP addresses for the captive portal.

These allowed DNS destination IP addresses are called a *whitelist*.

Each supported access point model can support up to 32 whitelists.

To effectively host captive portal pages on an external web server, the IP addresses of the destination web servers should be in the whitelist.

a Refer to the drop-down menu of existing **DNS Whitelist** entries to select a policy to be applied to this captive portal policy.

If no DNS Whitelist entries exist, select the **Create** or **Edit** icons and do the following.

For more information, see Setting the DNS Whitelist Configuration on page 799.

b If creating a new Whitelist, assign it a name up to 32 characters.

Use the **+ Add Row** button to populate the **Whitelist with Host** and **IP Index** values.

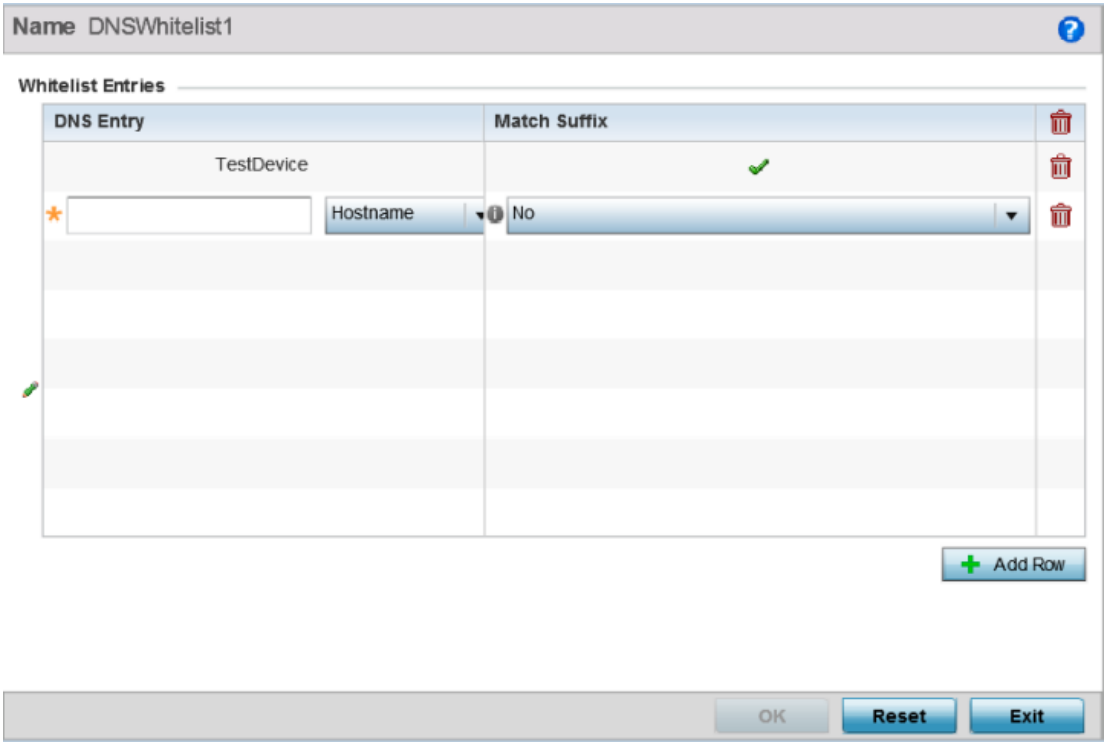



**Figure 376: Captive Portal Policy - Basic Configuration - Add DNS Whitelist Screen**

c Provide a numerical **IP address** or **Hostname** within the **DNS Entry** parameter for each destination IP address or host included in the whitelist.

d Use the **Match Suffix** parameter to match any hostname or domain name as a suffix.

The default setting is disabled.

e If necessary, select the radio button of an existing whitelist entry and select the **Delete** icon to remove the entry from the whitelist.

10 Set the following **Accounting** parameters to define how accounting is conducted for clients entering and exiting the captive portal.

Accounting is the method of collecting and sending security server information for billing, auditing and reporting user data; such as captive portal start and stop times, executed commands (such as PPP), number of packets and number of bytes. Accounting enables wireless network administrators to track captive portal services users are consuming.

| | |
|---|---|
| Enable RADIUS Accounting | Select this option to use an external RADIUS resource for AAA accounting. When selected, a AAA Policy field displays. This setting is disabled by default. |
| Enable Syslog Accounting | Select this option to log information about the use of remote access services by users using an external syslog resource. This information is of great assistance in partitioning local versus remote users. Remote user information can be archived to an external location for periodic network and user administration. This feature is disabled by default. |
| Syslog Host | When syslog accounting is enabled, use the drop-down menu to determine whether an IP address or Hostname is used as a syslog host. The IP address or hostname of an external server resource is required to route captive portal syslog events to that destination external resource destination. |
| Syslog Port | When syslog accounting is enabled, define the numerical syslog port the used to route traffic with the external syslog server. The default port is 514. |

11 Set the following **Data Limit** parameters values to define a data limit for clients accessing the network using the restrictions of a captive portal:

| | |
|---|---|
| Limit | Select this option to enable data limits for captive portal clients. Specify the maximum amount of data, in megabytes, allowed for each captive portal client. |
| Action | When a captive portal client reaches its data usage limit, a specified log action is executed. Choose from one of the following:<br>• **`Log Only`** — Logs the event<br>• **`log-and-disconnect`** — Logs the event and disconnects the user |

12 Set the **Logout FQDN** as the *fully qualified domain name* (FQDN) of the domain where the user will be redirected after logging out of the captive portal.

Example: `logout.guest.com`

13 Set the following **Localization** settings to add a URL to trigger a one-time redirect on demand.

The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.

| | |
|---|---|
| FQDN | Provide the FQDN address (for example, `local.guestaccess.com`) used to obtain localization parameters for a client. |
| Response | Enter a response message (512-character maximum) directed back to the client for localization HTTP requests. |

14 Refer to the Destination Ports for Redirection parameter (within the **Redirection Ports** field), and enter destination ports (separated by commas, or using a dash for a range) for consideration when re-directing client connections.

Standard ports 80 and 443 are always considered for client connections regardless of what's entered by the administrator.

15 Select **OK** to save the changes made within the Basic Configuration screen.

Select **Reset** to revert to the last saved configuration.

*Captive Portal Policy Web Page Configuration*

1 Select the **Web Page** tab to create locally or externally hosted HTML pages.

The Login page displays by default

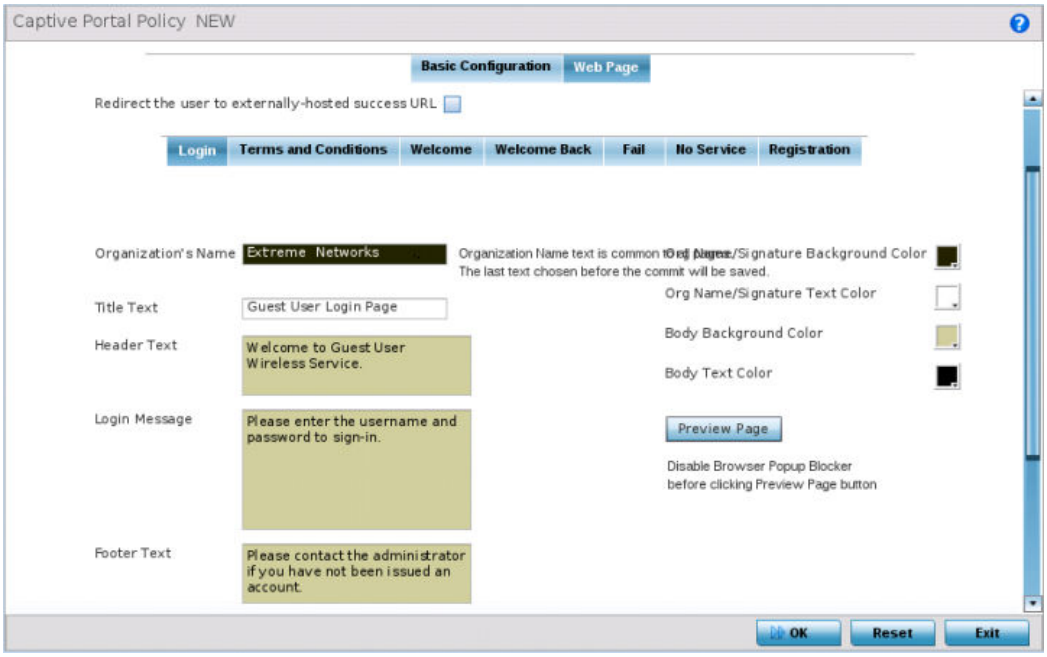



**Figure 377: Captive Portal Policy - Web Page - Internal Option Screen**

2 Refer to the following for information on the various captive portal Web pages:

The Login screen prompts the user for a username and password to access the captive portal and proceed to either the Terms and Conditions page (if used) or the Welcome page.

The Terms and Conditions page provides conditions that must be agreed to before captive portal access is permitted.

The Welcome page asserts a user has logged in successfully and can access the captive portal.

The Welcome Back page greets returning users.

The Fail page asserts authentication attempt has failed, the user is not allowed to access the internet (using this captive portal) and must provide the correct login information again to access the internet.

The No Service page asserts the captive portal service is temporarily unavailable for technical reasons. Once the services become available, the captive portal user is automatically connected back to the services available through the captive portal.

3 Select the location where the captive portal Login, Terms and Conditions, Welcome, Fail, No Service and Registration Web pages are hosted.

Available sources include Internal, External and Advanced. If Internal is selected, provide the information for each of the screens. If Advanced is selected, follow the on-screen instructions to upload custom Web pages. If **Externally hosted** is selected, provide the URLs for each of the necessary pages in the fields below.

| | |
|---|---|
| Organization Name | Set any organizational specific name or identifier which clients see during login. This setting is available only for the Login page. |
| Title Text | Set the title text displayed on the pages when wireless clients access captive portal pages. The text should be in the form of a page title describing the respective function of each page and should be unique to each function. |
| Header Text | Provide header text unique to the function of each page. |
| Login Message | Specify a message containing unique instructions or information for the users who access the Login, Terms and Condition, Welcome, Fail, No Service or Registration pages. In the case of the Terms and Agreement page, the message can be the conditions requiring agreement before captive portal access is permitted. |
| Footer Text | Provide a footer message displayed on the bottom of each page. The footer text should be any concluding message unique to each page before accessing the next page in the succession of captive portal Web pages. |
| Main Logo URL | The Main Logo URL is the URL for the main logo image displayed on each of the pages. Use the **Browse** button to navigate to the location of the target file. Optionally select the **`Use as banner`** option to designate the selected main logo as the page's banner as well. The banner option is disabled by default. |

| | |
|---|---|
| Small Logo URL | The Small Logo URL is the URL for a small logo image displayed on the screens. Use the **Browse** button to navigate to the location of the target file. |
| Signature | Provide the copyright and legal signature associated with the usage of the captive portal and the usage of the organization name provided. This setting is available only for the Login page. |

4 Refer to the right side of each screen to define how the **Org Name/Signature Background Color**, **Org/Name Signature Text Color**, **Body Background Color** and **Body Text Color** display for current screen.

Select the box to the right of each of these four items to launch a color palette where screen colors can be selected uniquely. Select **Preview Page** to review your color selections before committing the updates to captive portal screens. Each of the Login, Terms and Conditions, Welcome, Fail, No Service and Registration screens can have their background and signature colors set uniquely.

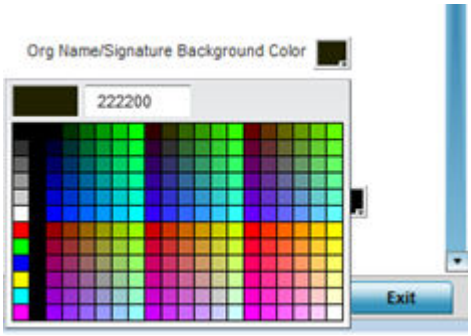



**Figure 378: Captive Portal Policy - Web Page - Color Palette Menu**

5 When setting the properties of the Registration screen, refer to the bottom portion of the screen to define email, country, gender, mobile, zip, street and name filters used as additional authentication criteria.

Guest users are redirected to the registration portal on association to the captive portal SSID. Users are displayed an internal (or) externally hosted registration page where the guest user must complete the registration process if not previously registered.

These fields are customizable to meet the needs of retailers providing guest access. The captive portal sends a message to the user (on the phone number or Email address provided at registration) containing an access code. The user inputs the access code and the captive portal verifies the code before returning the Welcome page and providing access. This allows a retailer to verify the phone number or Email address is correct and can be traced back to a specific individual.

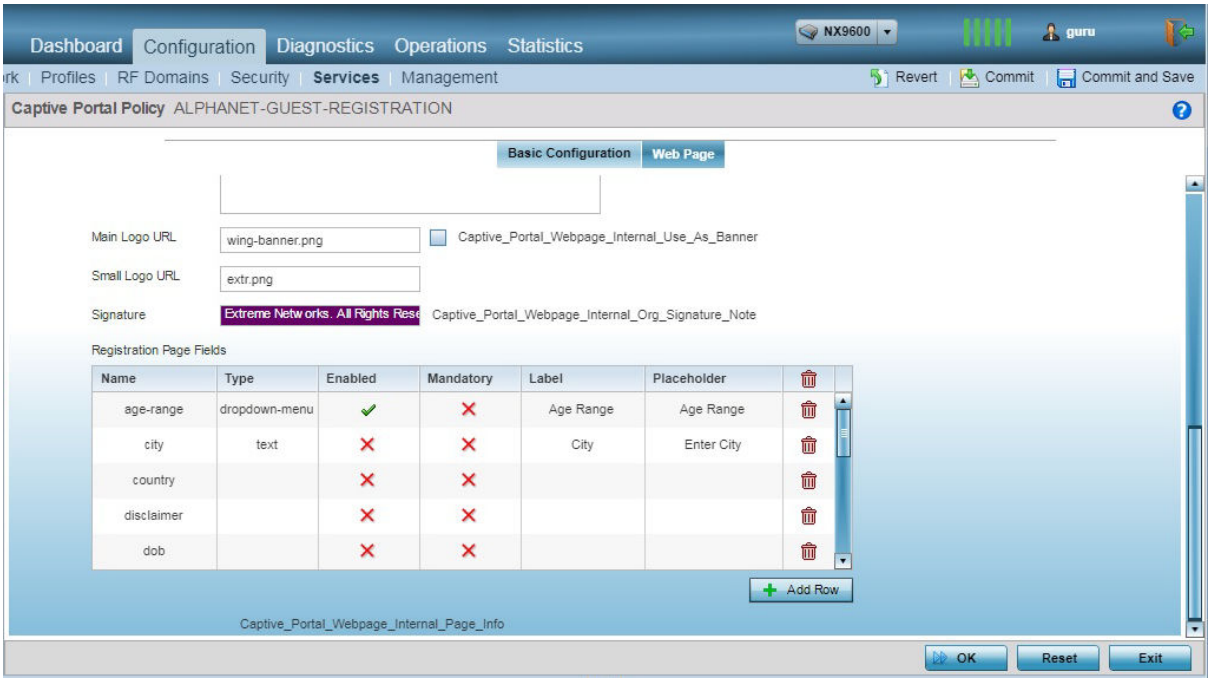



**Figure 379: Captive Portal Policy - Web Page - Internal - Registration - Registration Page Fields Table**

6 Click **OK** to save the changes made within any of the Internal Page screens.

Click **Reset** to revert to the last saved configuration.

7 If you are hosting the captive portal on an external system, select the **Externally Hosted** radio button.

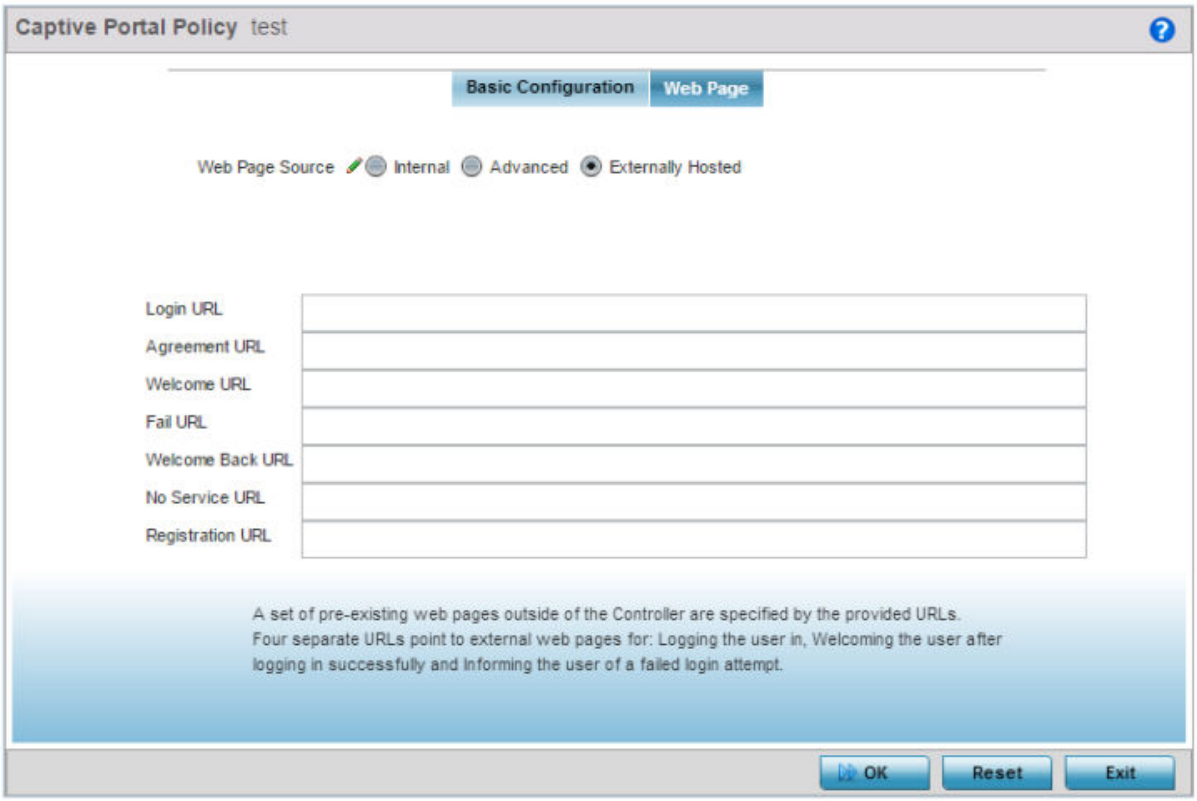



**Figure 380: Captive Portal Policy Screen - Web Page Tab - Externally Hosted Web Page Screen**

8 Set the following URL destinations for externally hosted captive portal pages:

| | |
|---|---|
| Login URL | Define the complete URL for the location of the Login page. The Login screen prompts the user for a username and password to access the Terms and Conditions or Welcome page. |
| Agreement URL | Define the complete URL for the location of the Terms and Conditions page. The Terms and Conditions page provides conditions that must be agreed to before wireless client access is provided. |
| Welcome URL | Define the complete URL for the location of the Welcome page. The Welcome page asserts the user has logged in successfully and can access resources via the captive portal. |
| Fail URL | Define the complete URL for the location of the Fail page. The Fail page asserts authentication attempt has failed, and the client cannot access the captive portal and the client needs to provide correct login information to regain access. |
| Welcome Back URL | Define the complete URL for the location of the Welcome Back page. The Welcome Back page asserts the user has re-logged in successfully and can access resources via the captive portal. |

| | |
|---|---|
| No Service URL | Define the complete URL to the location of the No Service page. The No Service URL is needed by users encountering difficulties connecting to the external resource used to host the captive portal pages. |
| Registration URL | Define the complete URL to the location of the Registration page. The Registration page is displayed to new users to register (provide user information) in order to access the captive portal managed Internet resources. |

9 Click **OK** when completed to update the captive portal policy settings.

Click **Reset** to revert to the last saved configuration.

10 Select **Advanced** to use a custom-developed directory of web pages.

Web pages in the directory can be copied to and from the access point, to support the captive portal.

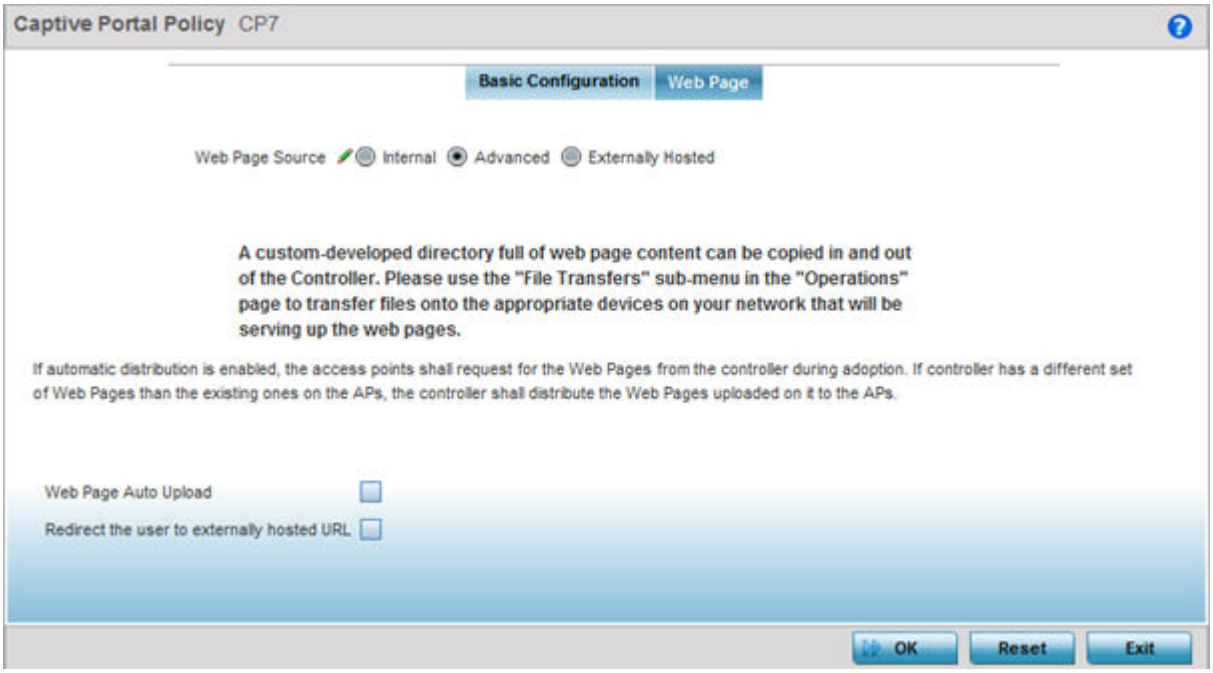



**Figure 381: Captive Portal Policy - Web Page Screen - Advanced Option**

11 The access point maintains its own set of Advanced web pages for custom captive portal creation.

Refer to **Operations** > **Devices** > **File Transfers** and use the **Source** and **Target** fields to move captive portal pages as needed to managed devices that may be displaying and hosting captive portal connections.

Select the **Web Page Auto Upload** check box to enable automatic upload of captive portal Web pages.

Select the **Redirect the user to externally-hosted success URL** check box, if the Welcome page is externally hosted.

12 Click **OK** when completed to update the captive portal's advanced configuration.

Click **Reset** to revert the screen back to its last saved configuration.

## Setting the DNS Whitelist Configuration

A DNS whitelist is used in conjunction with a captive portal to provide captive portal services to wireless clients. Use the DNS whitelist parameter to create a set of allowed destination IP addresses within the captive portal. These allowed IP addresses are called the Whitelist. To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist. Each supported access point model can support up to 32 whitelists, with the exception of AP6521 model which can only support up to 16 whitelists.

To define a DNS whitelist:

1 Select **Configuration** > **Services** > **DNS Whitelist**.

The DNS Whitelist screen displays those existing whitelists available to a captive portal.

2 Select **Add** to create a whitelist, **Edit** to modify a selected whitelist, or **Delete** to remove a whitelist.

3 To create a whitelist, assign it a name up to 32 characters.

Use the **+ Add Row** button to populate the whitelist table with Host and IP Index parameters that must be defined for each whitelist entry.

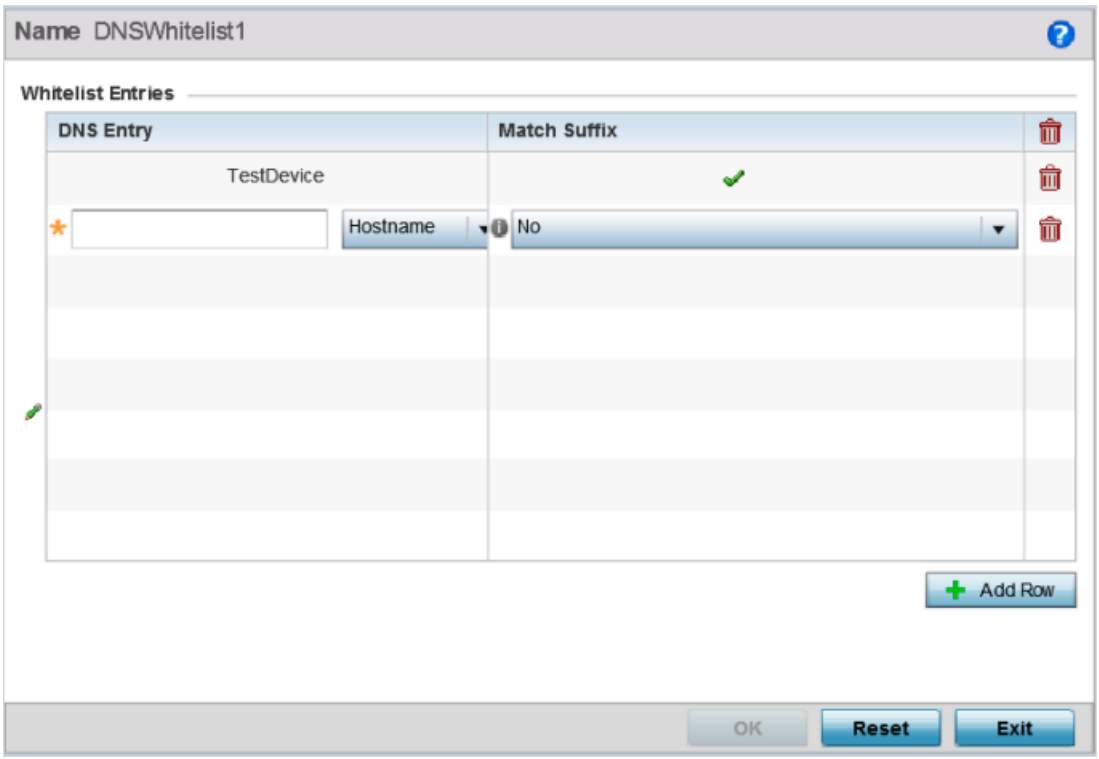



**Figure 382: DNS Whitelist Screen**

4 Provide a numerical IP address or Hostname within the DNS Entry parameter for each destination IP address or host in the whitelist.

5 Use the Match Suffix parameter to match any hostname or domain name as a suffix.

The default setting is disabled.

6 If necessary, select the radio button of an existing whitelist entry and select the **- Delete** icon to remove the entry from the whitelist.

7 Click **OK** when completed to update the whitelist screen.

Click **Reset** to revert the screen to its last saved configuration.

## Setting the DHCP Configuration

*Dynamic Host Configuration Protocol* (DHCP) allows hosts on an IP network to request and be assigned IP addresses and discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the onboard DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an pre-determined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The DHCP server ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not yet expired). Therefore, IP address management is conducted by the internal DHCP server, not by an administrator.

WiNG managed access points have an internal DHCP server resource. However, the AP6521 model does not have an onboard DHCP server resource and an external resource must be used.

The internal DHCP server groups wireless clients based on defined user-class options. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined). Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnet. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned.

Refer to the following sections for more information on configuring DHCP parameters:

- Defining DHCP Pools on page 802
- Defining DHCP Server Global Settings on page 810
- DHCP Class Policy Configuration on page 812
- DHCP Deployment Considerations on page 813

To access and review the local DHCP server configuration:

1 Select **Configuration** > **Services** > **DHCP Server Policy**.

The DHCP Server screen displays. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are then compared against classes.

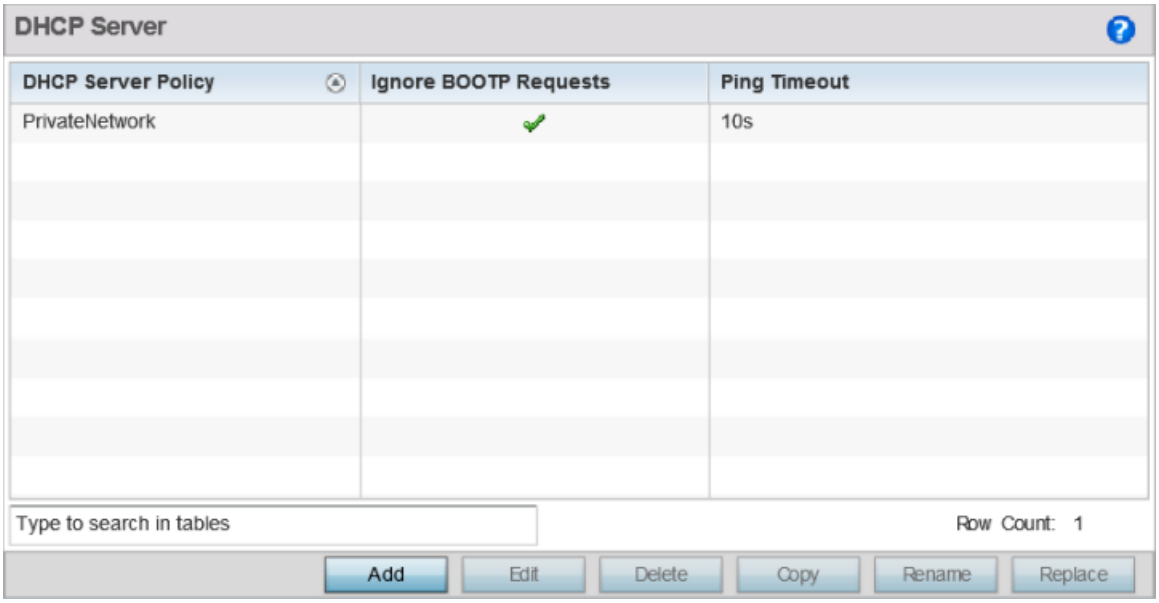



**Figure 383: DHCP Server Policy Screen**

2 Review the following DHCP server configurations (at a high level) to determine whether a new server policy requires creation, an existing policy requires modification or an existing policy requires deletion.

| | |
|---|---|
| DHCP Server Policy | Lists the name assigned to each DHCP server policy when it was initially created. The name assigned to a DHCP server policy cannot be modified as part of the policy edit process. However, obsolete policies can be deleted as needed. |
| Ignore BOOTP Requests | A green checkmark within this column means this policy has been set to ignore BOOTP requests. A red "X" defines the policy as accepting BOOTP requests. BOOTP (boot protocol) requests boot remote systems within the controller or service platform managed network. BOOTP messages are encapsulated inside UDP messages and are forwarded by the controller or service platform. This parameter can be changed within the DHCP Server Global Settings screen. |
| Ping Timeout | Lists the interval (from 1 -10 seconds) for a DHCP server ping timeout. The timeout is used to intermittently ping and discover whether a client requested IP address is already in use. This parameter can be changed within the DHCP Server Global Settings screen. |

3 Click **Add** to create a new DHCP server policy, choose an existing policy and click **Edit** to modify the policy's properties, or choose an existing policy and click **Delete** to remove the policy from those available.

Adding or Editing a DHCP server policy displays the DHCP Server Policy screen by default. Click **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

## Defining DHCP Pools

A *pool* (or range) of IP network addresses and DHCP options can be created for each IP interface configured. This range of addresses can be made available to DHCP enabled wireless devices on either a permanent or leased basis. DHCP options are provided to each DHCP client with a DHCP response and provide DHCP clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCP client.

To define the parameters of a DHCP pool:

1 Select **Configuration** > **Services**.

2 Select **DHCP Server Policy**.

The DHCP Server Policy screen displays the DHCP Pool tab by default.

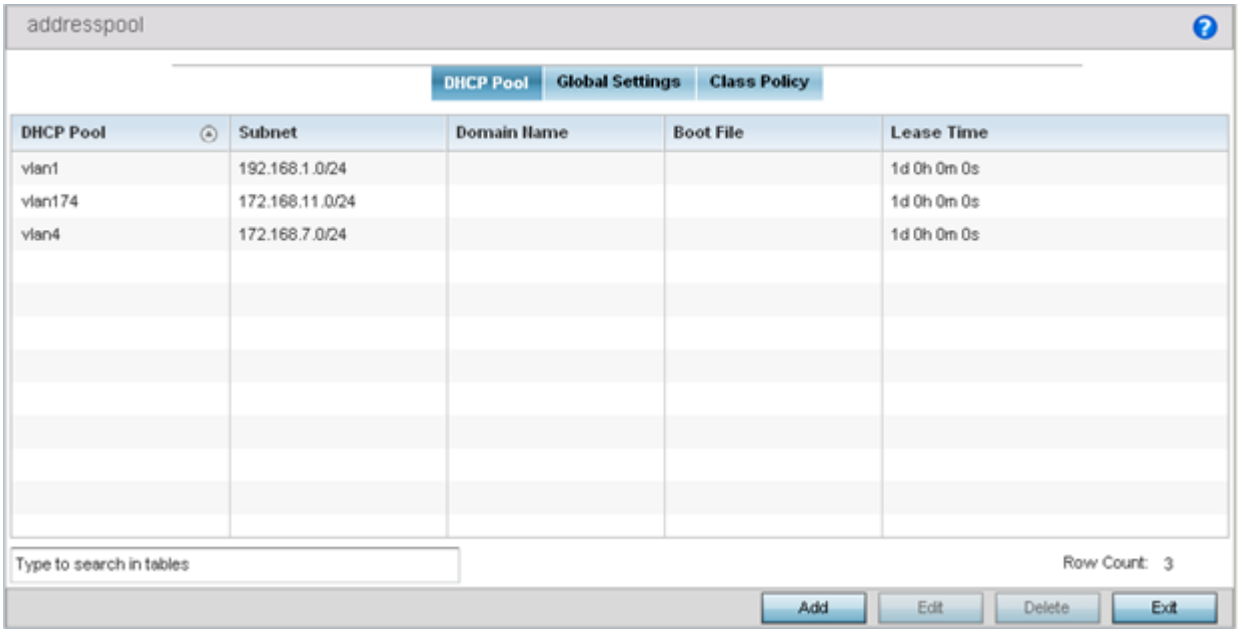



**Figure 384: DHCP Server Policy - Add/Edit - DHCP Pool Tab**

3 Review the following DHCP pool configurations to determine if an existing pool can be used as is, a new one requires creation or edit, or a pool requires deletion:

| | |
|---|---|
| DHCP Pool | Displays the name assigned to the network pool when created. The DHCP pool name represents the group of IP addresses used to assign to DHCP clients upon request. The name assigned cannot be modified as part of the edit process. However, if the network pool configuration is obsolete it can be deleted. |
| Subnet | Displays the network address and mask used by clients requesting DHCP resources. |
| Domain Name | Displays the domain name defined used with this network pool. *Domain Name Services* (DNS) converts human-readable host names into IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A *fully qualified domain name* (FQDN) consists of a host name plus a domain name. For example, *computername.domain.com*. |

| | |
|---|---|
| Boot File | Boot files (*Boot Protocol*) are used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages, so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed. |
| Lease Time | If a lease time has been defined for a listed network pool, it displays in an interval from 1 - 9,999,999 seconds. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another requesting DHCP client. |

4 Select **Add** to create a new DHCP pool, **Edit** to modify an existing pool's properties or **Delete** to remove a pool from among those available.

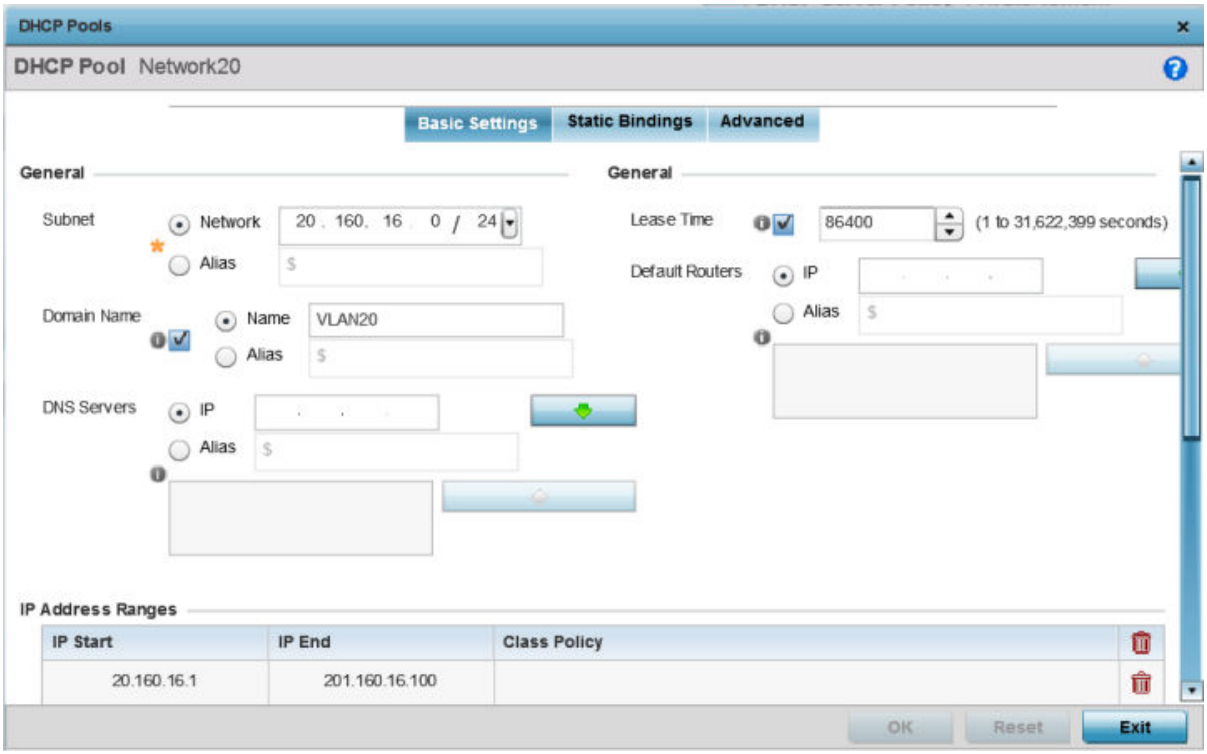



**Figure 385: DHCP Pools - Add/Edit - Basic Settings Tab**

If you are adding or editing a DHCP pool, the DHCP Pool screen displays the Basic Settings tab by default. Define the required parameters for the Basic Settings, Static Bindings and Advanced tabs to complete the creation of the DHCP pool.

5 Set the following **General** parameters, or aliases, from within the Basic Settings tab.

| | |
|---|---|
| DHCP Pool | If adding a new pool, a name is required. The pool is the range of IP addresses defined for DHCP assignment or lease. The name assigned cannot be modified as part of the edit process. However, if the network pool configuration is obsolete it can be deleted. The name cannot exceed 32 characters. |
| Subnet | Define the IP address/Subnet Mask or IP alias used for DHCP discovery and requests between the local DHCP server and clients. The IP address and subnet mask (or its alias) are required to match the addresses of the layer 3 interface for the addresses to be supported through that interface.<br>Select **Alias** to use a network alias with the subnet configuration. For more information, see Alias on page 708. |

| | |
|---|---|
| Domain Name | Provide the domain name or domain alias used with this pool. Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A *fully qualified domain name* (FQDN) consists of a host name plus a domain name. For example, *computername.domain.com*.<br>Select **Alias** to use a string alias with the domain name configuration. For more information, see Alias on page 708. |
| DNS Servers | Define one (or a group) of Domain Name Servers (DNS) to translate domain names to IP addresses.<br>Select **Clear** to remove any single IP address as needed. Up to eight IP addresses can be supported. Select **Alias** to use a host alias with the DNS servers configuration. For more information, see Alias on page 708. |
| Lease Time | DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address within the defined time, that IP address can be re-assigned to another DHCP supported client. Select this option to assign a lease in either Seconds (1 - 31,622,399), Minutes (1 - 527,040), Hours (1 - 8,784) or Days (1 - 366). The default setting is enabled, with a lease time of 1 day. |
| Default Routers | After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address or IP alias for one or more routers used to map host names into IP addresses for clients. Up to eight default router IP addresses are supported. If setting a default router IP alias, ensure it begins with a dollar sign ($) and does not exceed 32 characters. An actual router IP address is the default setting, not an alias.<br>Select **Alias** to use a hoast alias with the default routers configuration. For more information, see Alias on page 708. |

6 Define the range of included (starting and ending IP addresses) addresses for this particular pool.

Use the **IP Address Ranges** and **Excluded IP Address Ranges** fields for this operation.

a Select the **+ Add Row** button at the bottom of the IP addresses field to add a new range.

Select the radio button of an existing IP address range and select the **Delete** icon to remove it from the list of those available.

b Enter a viable range of IP addresses in the **IP Start** and **IP End columns**.

This is the range of addresses available for assignment to requesting clients.

c Select the **Create** icon or the **Edit** icon within the **Class Policy** column to display the DHCP Server Policy screen if a class policy is not available from the drop-down menu.

7 Refer to the **Excluded IP Address Range** field and select the **+Add Row** button.

Add ranges of IP address to exclude from lease to requesting clients. Having ranges of unavailable addresses is a good practice to ensure IP address resources are in reserve. Select the **Delete** icon as needed to remove an excluded address range.

8 Click **OK** to save the updates to the DHCP Pool Basic Settings tab.

Click **Reset** to revert to the last saved configuration.

9 Select the Static Bindings tab from within the DHCP Pools screen.

A binding is a collection of configuration parameters, including an IP address, associated with, or bound to, a DHCP client. Bindings are managed by DHCP servers. DHCP bindings automatically map a device MAC address to an IP address using a pool of DHCP supplied addresses. Static bindings assign IP addresses without creating numerous host pools with manual bindings. Static host bindings use a text file the DHCP server reads. It eliminates the need for a lengthy configuration file and reduces the space required to maintain address pools.

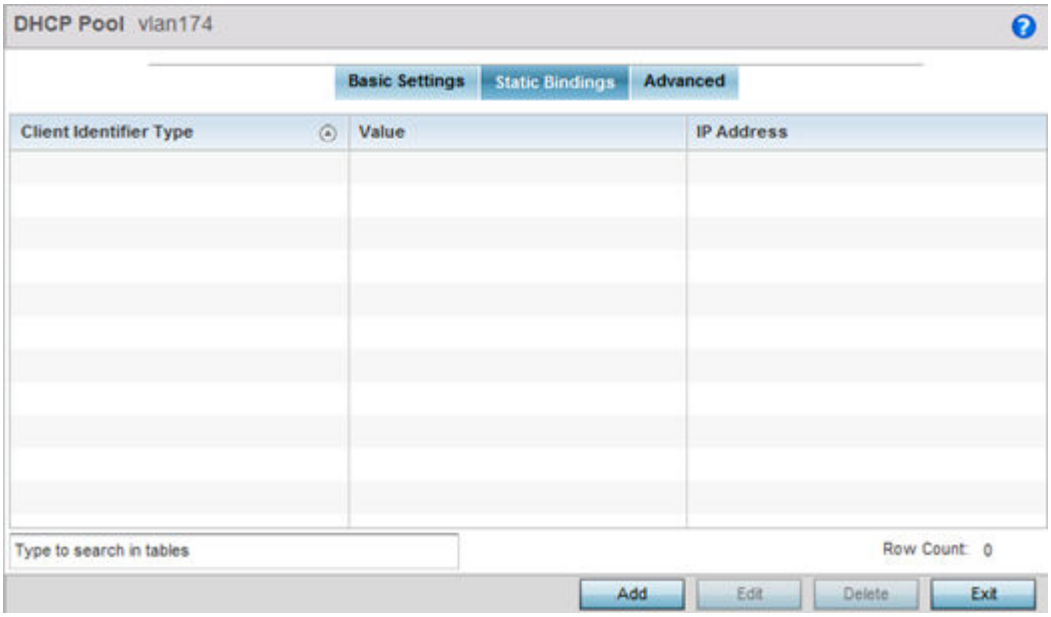



**Figure 386: DHCP Pools - Add/Edit - Static Bindings Tab**

10 Review existing DHCP pool static bindings to determine if a static binding can be used as is, if a new binding requires creation or edit, or if a binding requires deletion:

| | |
|---|---|
| Client Identifier Type | Whether the reporting client is using a hardware address or client identifier as its identifier type within requests to the DHCP server. |
| Value | The hardware address or client identifier assigned to the client when added or last modified. |
| IP Address | The IP address of the client on this interface that's currently using the pool name listed. |

11 Click **Add** to create a new static binding configuration, **Edit** to modify an existing static binding configuration or **Delete** to remove a static binding from among those available.

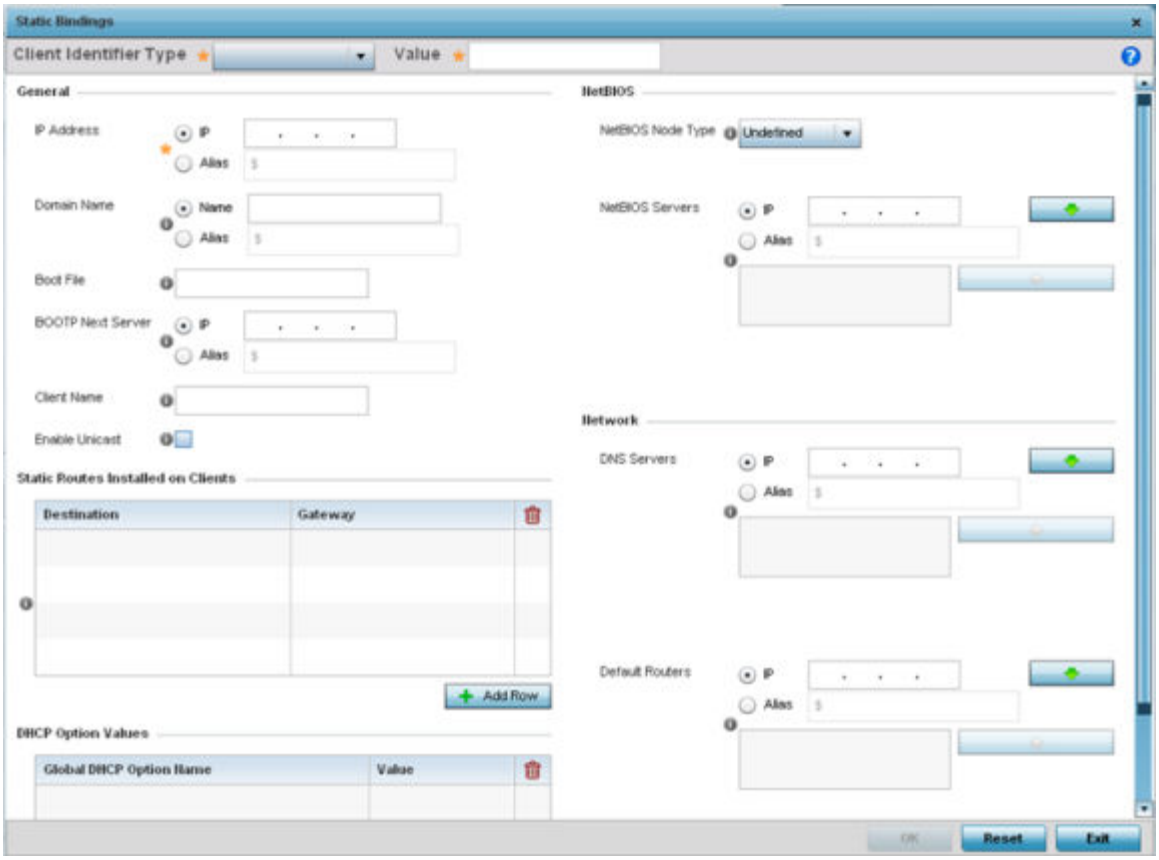



**Figure 387: DHCP Pools - Add/Edit - Static Bindings - Add Screen**

12 Set the following **General** parameters or aliases to complete the creation of the static binding configuration.

| | |
|---|---|
| Client Identifier Type | Use the drop-down menu whether the DHCP client is using a Hardware Address or Client Identifier as its identifier type with a DHCP server. |
| Value | Provide a hardware address or client identifier value to help differentiate the client from other client identifiers. |
| IP Address | Set the IP address of the client using this host pool. Select **Alias** to use a network alias with the IP address configuration. For more information, see Alias on page 708. |
| Domain Name | Provide a domain name for the current interface. Domain names are not case sensitive and can contain letters, numbers, and hyphens. A *fully qualified domain name* (FQDN) consists of a host name plus a domain name. For example, *computername.domain.com*.<br>Select **Alias** to use a string alias with the domain name configuration. For more information see Alias on page 708. |
| Boot File | Enter the name of the boot file used with this pool. Boot files (Boot Protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed. |

| | |
|---|---|
| BOOTP Next Server | Provide the numerical IP address or alias of the server providing BOOTP resources. Select **Alias** to use a network alias with the BOOTP Next Server configuration. For more information see Alias on page 708. |
| Client Name | Provide the name of the client requesting DHCP Server support. |
| Enable Unicast | Unicast packets are sent from one location to another location (there is just one sender and one receiver). Select this option to forward unicast messages to just a single device within this network pool. This setting is disabled by default. |

13 Define the following **NetBIOS** parameters to complete the creation of the static binding configuration:

| | |
|---|---|
| NetBIOS Node Type | Set the NetBIOS Node Type used with this particular pool. The following options are available:<br>• Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name.<br>• Peer-to-Peer - Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.<br>• Mixed - A mixed node using broadcast queries to find a node, and failing that, queries a known p-node name server for the address.<br>• Hybrid - A combination of two or more nodes.<br>• None - No node type is applied. |
| NetBIOS Servers | Specify a numerical IP address of a single NetBIOS WINS server or a group of servers available to requesting clients. A maximum of eight server IP addresses can be assigned.<br>Select **Alias** to use a network alias with the NetBIOS server configuration. For more information see Alias on page 708. |

14 Refer to the **Static Routes Installed on Clients** field to set Destination IP and Gateway addresses enabling the assignment of static IP addresses without creating numerous host pools with manual bindings.

This eliminates the need for a long configuration file and reduces the space required in NVRAM to maintain address pools. Select the **+ Add Row** button to add individual destinations. Select the Delete icon to remove it from the list of those available.

15 Refer to the **DHCP Option Values** table to set Global DHCP options.

A set of global DHCP options applies to all clients, whereas a set of subnet options applies only to the clients on a specified subnet. If you configure the same option in more than one set of options, the precedence of the option type decides which the DHCP server supports a client.

a Select the **+ Add Row** button to add individual options.

Assign each one a **Global DHCP Option Name** to help differentiate it from others with similar configurations. Select the radio button for an existing option and select the **- Delete** button to remove it from the list of those available.

b Assign a Value to each option with codes from 1 through 254.

A vendor-specific option definition only applies to the vendor class for which it is defined.

16 In the **Network** field, define one or more of DNS Servers and Default Routers to translate domain names to IP addresses.

Up to eight IP addresses can be provided. The IP option is selected by default for both DNS Servers and Default Routers. foo

Select **Alias** to use a network alias with the DNS server configuration.. For more information see Alias on page 708.

17 Click **OK** when completed to update the static bindings configuration.

Click **Reset** to revert the screen back to its last saved configuration.

18 Select the Advanced tab to define additional NetBIOS and Dynamic DNS parameters.

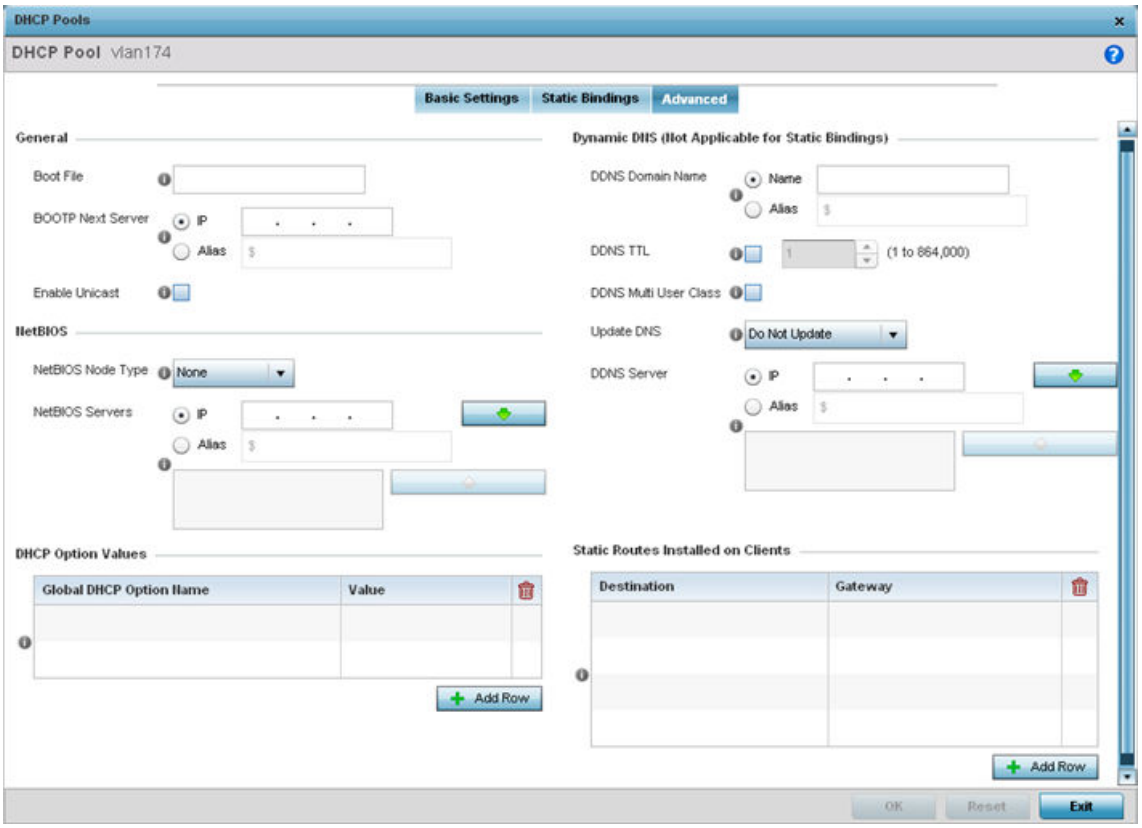



**Figure 388: DHCP Pools - Add/Edit - Advanced Tab**

19 To add or modify the DHCP pool's advanced settings, set the following General parameters:

| | |
|---|---|
| Boot File | Enter the name of the boot file used with this pool. Boot files (boot protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each pool can use a different file as needed. |
| BOOTP Next Server | Provide the numerical IP address or alias of the server providing BOOTP resources. Select **Alias** to use a network alias with the BOOTP Next Server configuration. For more information see Alias on page 708. |
| Enable Unicast | Unicast packets are sent from one location to another location (there's just one sender, and one receiver). Select this option to forward unicast messages to just a single device within the network pool. This setting is disabled by default. |

20 Set the following **NetBIOS** parameters for the network pool:

| | |
|---|---|
| NetBIOS Node Type | Set the NetBIOS Node Type used with this particular pool. The following options are available:<br>• Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name.<br>• Peer-to-Peer - Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.<br>• Mixed - Mixed uses broadcast queries to find a node, and failing that, queries a known p-node name server for the address.<br>• Hybrid - A combination of two or more nodes.<br>• None - No NetBIOS node type is applied. |
| NetBIOS Servers | Specify a numerical IP address of a single NetBIOS WINS server or a group of servers available to requesting clients. A maximum of eight server IP addresses can be assigned.<br>Select **Alias** to use a network alias with the NetBIOS server configuration. For more information see Alias on page 708. |

21 Refer to the **DHCP Option Values** table to set Global DHCP options applicable to all clients, whereas a set of subnet options applies only to the clients on a specified subnet.

a Select the **+ Add Row** button to add individual options.

Assign each a Global DHCP Option Name to help differentiate it from others with similar configurations. Select the radio button of an existing option and select **Delete** to remove it from the list.

b Assign a Value to each option from 1 through 254.

A vendor-specific option definition applies only to the vendor class for which it is defined.

22 Define the following set of **Dynamic DNS (Not Applicable for Static Bindings)** parameters used with the network pool configuration.

Using DDNS controllers and service platforms can instruct a DNS server to change, in real time (ad hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

| | |
|---|---|
| DDNS Domain Name | Enter a domain name for DDNS updates representing the forward zone in the DNS server. For example, *test.net*. The **Name** option is selected by default. Optionally select **Alias** to provide a DDNS domain name alias beginning with a dollar sign ($) and not exceeding 32 characters. |
| DDNS TTL | Select this option to set a TTL (Time to Live) to specify the validity of DDNS records. The maximum value configurable is 864000 seconds. |
| DDNS Multi User Class | Select the check box to associate the user class option names with a multiple user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options. |

| | |
|---|---|
| Update DNS | Set if DNS is updated from a client or a server. Select either **`Do Not Update`**, **`Update from Server`**, or **`Update from Client`**. The default setting is **`Do Not Update`**, implying that no DNS updates occur at all. |
| DDNS Server | Specify a numerical IP address of one or two DDNS servers. Dynamic DNS (DDNS) prompts a computer or network to obtain a new IP address lease and dynamically associate a hostname with that address, without having to manually enter the change every time. Since there are situations where an IP address can change, it helps to have a way of automatically updating hostnames that point to the new address every time. The IP option is selected by default. Optionally select **Alias** to provide a DDNS server IP alias beginning with a dollar sign ($) and not exceeding 32 characters. |

23 Refer to the **Static Routes Installed on Clients** table to set fixed routes for client destination and gateways.

Select the **+ Add Row** button to add individual options for Destination and Gateway addresses.

24 Click **OK** to save updates to the DHCP pool's Advanced settings.

Click **Reset** to revert the screen to its last saved configuration.

## Defining DHCP Server Global Settings

Set a DHCP server global configuration by defining whether BOOTP requests are ignored and by defining DHCP global server options.

To define DHCP server global settings:

1 Select the Global Settings tab and ensure that the **Activate DHCP Server Policy** button remains selected.

This option must remain selected to implement the configuration as part of the access point profile.

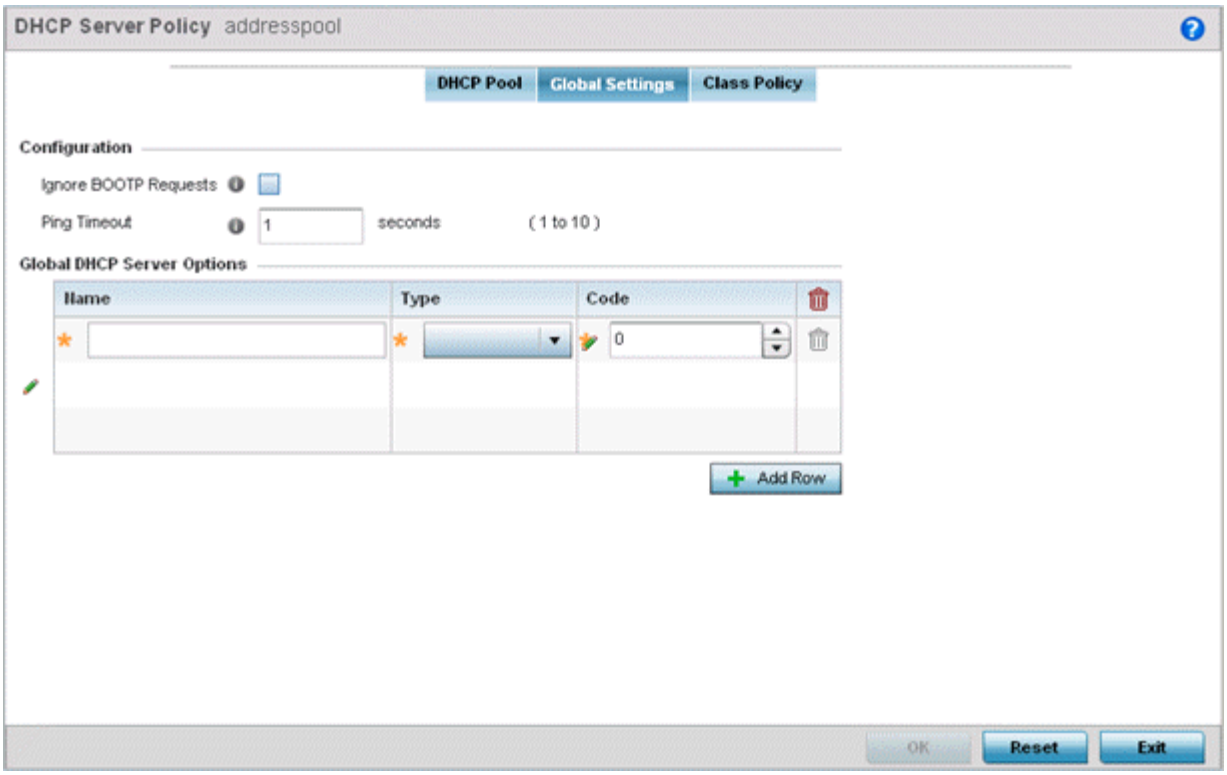



**Figure 389: DHCP Server Policy - Add/Edit - Global Settings Tab**

2 Set the following parameters within the **Configuration** field:

| | |
|---|---|
| Ignore BOOTP Requests | Select the check box to ignore BOOTP requests. BOOTP (boot protocol) requests boot remote systems within the network. BOOTP messages are encapsulated inside UDP messages and forwarded. This feature is disabled by default, so unless selected, BOOTP requests are forwarded. |
| Ping Timeout | Set an interval (from 1 -10 seconds) for the DHCP server ping timeout. The timeout is the intermittent ping and discover interval to determine whether a client requested IP address is already used. |

3 Set the **Activation Criteria** for the DHCP server policy:

Use the drop-down menu to select the criteria from one of **`none`**, **`vrrp-master`**, **`cluster-master`** or **`rf-domain-manager`**. The default value is **`none`**.

4 Refer to the **Global DHCP Server Options** field.

a Use the **+ Add Row** button at the bottom of the field to add a new global DHCP server option.

Select the radio button of an existing global DHCP server option and select the Delete icon to remove it from the list of those available.

b Use the **Type** drop-down menu to specify whether the DHCP option is being defined as a numerical IP address, an ASCII string, or a hex string.

Highlight an entry from within the Global Options screen and click the **Remove** button to delete the name and value.

5 Click **OK** to save the updates to the DHCP server global settings.

Click **Reset** to revert the screen to its last saved configuration.

## DHCP Class Policy Configuration

A controller, service platform or Access Point's local DHCP server assigns IP addresses to requesting DHCP clients based on user class option names. The DHCP server can assign IP addresses from as many IP address ranges as defined by an administrator. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

Refer to the DHCP Class Policy screen to review existing DHCP class names and their current multiple user class designations. Multiple user class options enable a user class to transmit option values to DHCP servers supporting multiple user class options. Either add a new class policy, edit the configuration of an existing policy or permanently delete a policy as required.

To review DHCP class policies:

1 Select the **Class Policy** tab and ensure that the **Activate DHCP Server Policy** button remains selected.

This option must remain selected to implement the configuration as part of the access point profile.

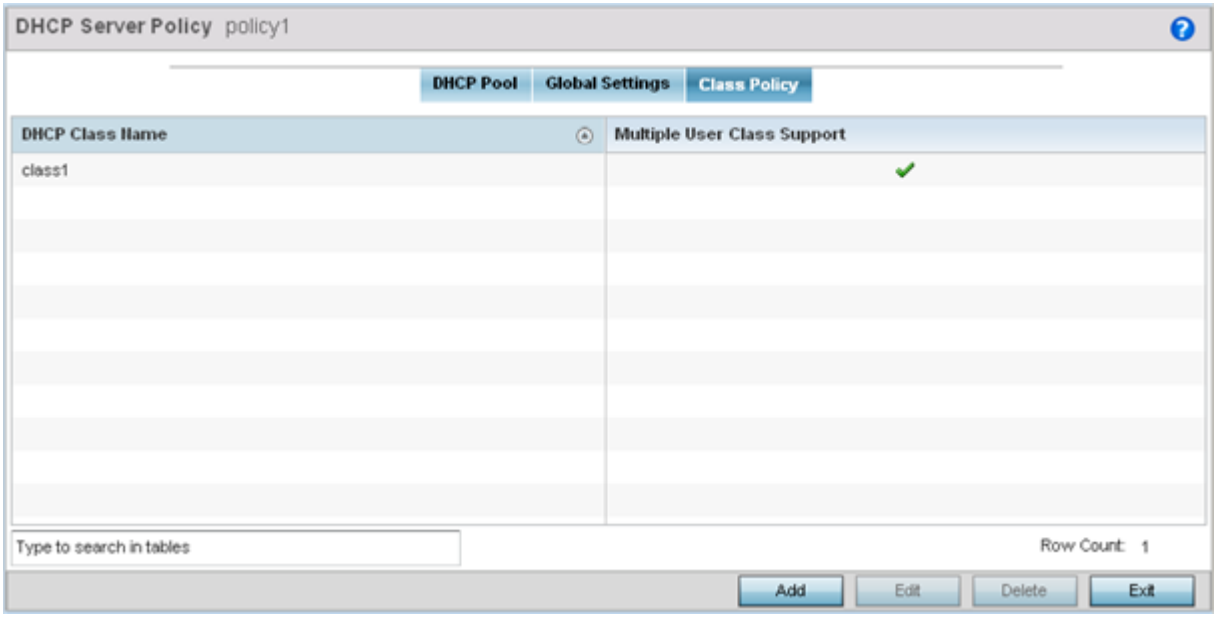



**Figure 390: DHCP Server Policy - Class Policy Tab**

2 Click **Add** to create a new DHCP class policy, **Edit** to update an existing policy or **Delete** to remove an existing policy.

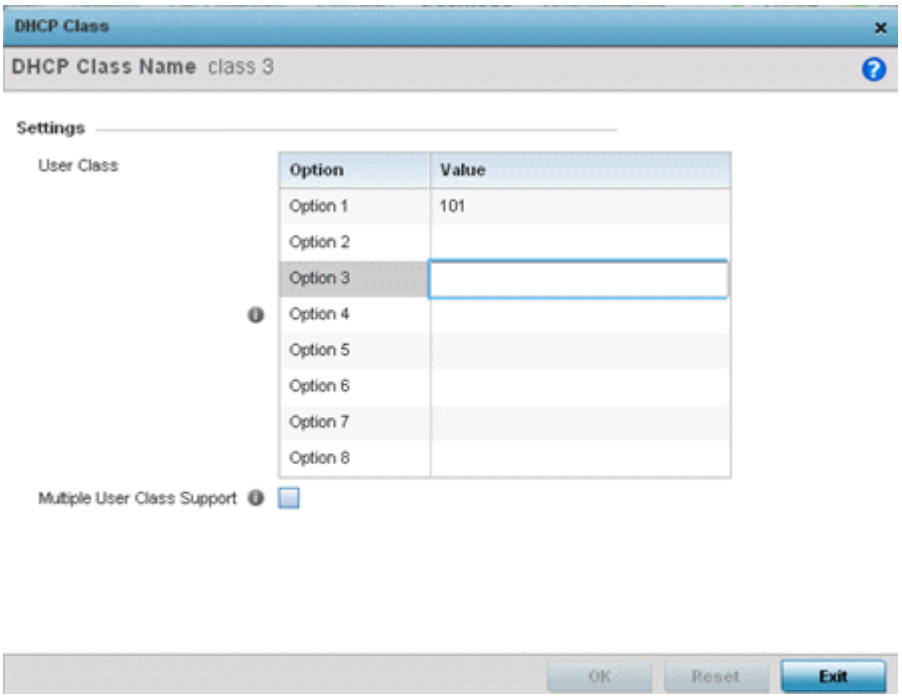



**Figure 391: DHCP Class Name Add Screen**

3 If you are adding a new DHCP Class Name, assign a name representative of the device class supported.

The DHCP user class name should not exceed 32 characters.

4 Select a row within the **Value** column to enter a 32-character maximum value string.

5 Select **Multiple User Class** to enable multiple option values for the user class.

This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options.

6 Click **OK** to save the updates to this DHCP class policy.

Click **Reset** to revert the screen to its last saved configuration.

## DHCP Deployment Considerations

Before defining an DHCP server configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- DHCP option 189 is required when AP650 model access points are deployed over a layer 3 network and require layer 3 adoption. DHCP services are not required for AP650 access points connected to a VLAN that's local to the controller or service platform.
- DHCP's lack of an authentication mechanism means a DHCP server cannot check if a client or user is authorized to use a given user class. This introduces a vulnerability when using user class options. For example, if a user class is used to assign a special parameter (for example, a database server), there is no way to authenticate a client and it's impossible to check if a client is authorized to use this parameter.

- Ensure that traffic can pass on UDP ports 67 and 68 for clients receiving DHCP information.

## Setting the Bonjour Gateway Configuration

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates the devices (printers, computers etc.) and services these computers provide over a local network.

Bonjour provides a method to discover services on a local area network (LAN). Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

Note
Up to eight (8) Bonjour discovery policies can be configured.

The following options can be configured:

- Configuring a Bonjour Discovery Policy
- Configuring a Bonjour Forwarding Policy

Note
The WiNG 7.1 release does not support Bonjour on AP505 and AP510 model access points. This feature will be supported in future releases.

### Configuring a Bonjour Discovery Policy

The Bonjour discovery policy configures how Bonjour services are located. It configures the VLANs on which these services can be found.

Note
The WiNG 7.1 release does not support Bonjour on AP505 and AP510 model access points. This feature will be supported in future releases.

To display Bonjour discovery policy information:

1 Select **Configuration**.
2 Select **Services**.
3 Select **Bonjour Gateway** to expand its submenu.

4 Select **Discovery Policy**.

The Discovery Policy screen displays the name of the configured Bonjour discovery policies.

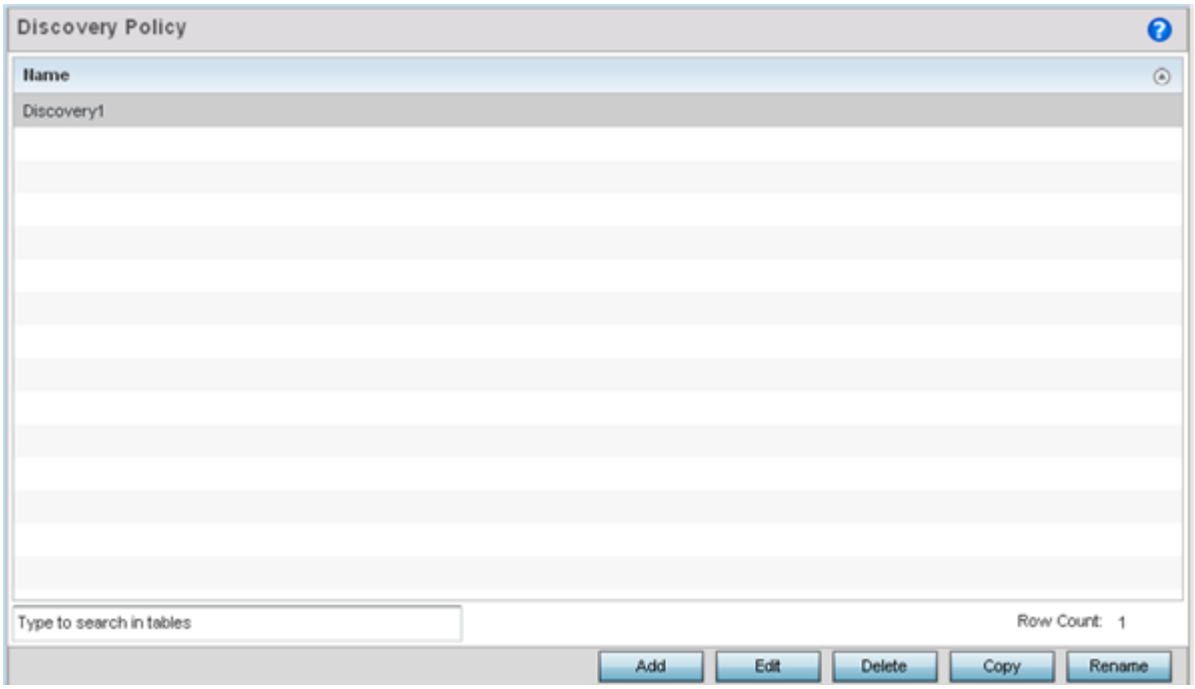



**Figure 392: Bonjour Gateway - Discovery Policy Screen**

5 Select an existing policy and select **Edit** to modify its configuration or select **Add** to create a new configuration..

Select an existing policy and click **Delete** to delete the policy, or use **Copy** to create a copy of a policy for further modifications. Optionally, **Rename** a policy or **Copy** a policy to a different location.

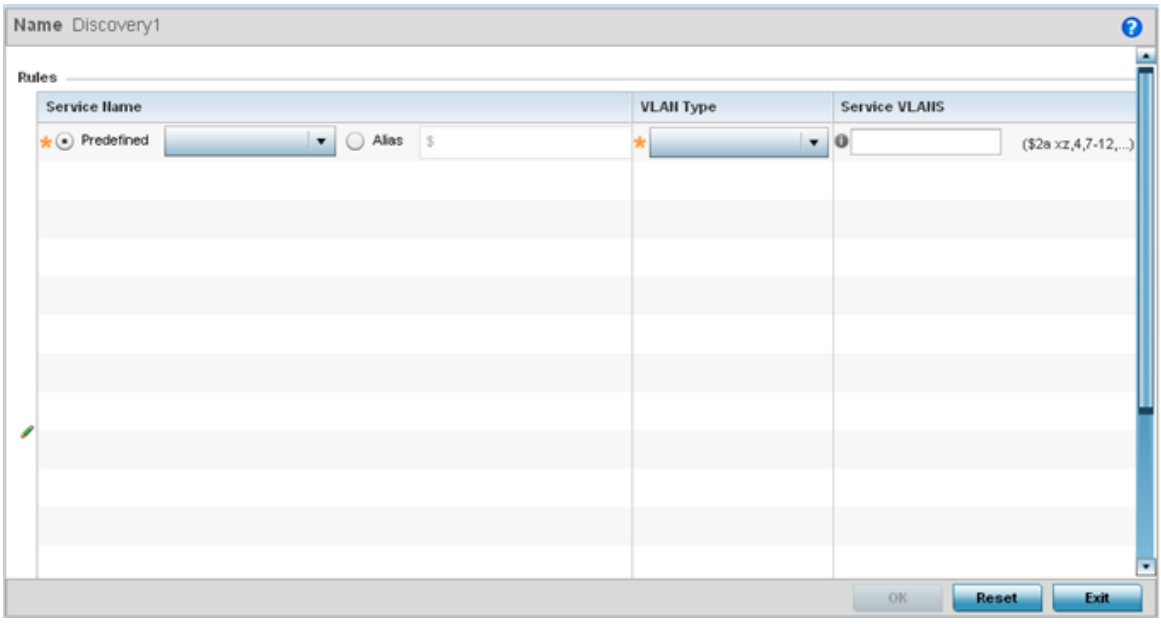



**Figure 393: Bonjour - Discovery Policy - Add/Edit Policy Screen**

6 Select the **+ Add Row** button to add a rule to the Bonjour discovery policy.

These are the services discoverable by the Bonjour gateway.

7 Set the following discovery attributes for the discovery policy configuration:

| | |
|---|---|
| Service Name | Define the service that can be discovered by the Bonjour gateway.<br>• Predefined – Use the drop-down menu to select from a list of predefined Apple services (Scanner, Printer, HomeSharing etc.).<br>• Alias – Use an existing alias to define a service that is not available in the predefined list. |
| VLAN Type | Use the drop-down menu to select the VLAN type.<br>• **`local`** – The VLAN(s) defined in the **Service VLAN** field use a local bridging mode.<br>• **`tunneled`** – The VLAN(s) defined in the **Service VLAN** field are shared tunnel VLANs. |
| Service VLANs | Provide a VLAN or a list of VLANs on which the selected service is discoverable. |

8 Click **OK** to save updates to this Bonjour Discovery policy.

Click **Reset** to revert the screen to its last saved configuration.

## Configuring a Bonjour Forwarding Policy

A Bonjour forwarding policy enables the discovery of services on VLANs not visible to the device running the Bonjour Gateway. Bonjour forwarding enables the forwarding of Bonjour advertisements across VLANs to enable the Bonjour gateway to build a list of services and VLANs where services are available.

Note
Only one (1) Bonjour forwarding policy is configurable.

Note
There must be Layer 2 connectivity between devices for forwarding to work.

Note
The WiNG 7.1 release does not support Bonjour on AP505 and AP510 model access points. This feature will be supported in future releases.

To display Bonjour forwarding policy information:

1 Select **Configuration**.
2 Select **Services**.
3 Select **Bonjour Gateway** to expand its submenu.

4 Select **Forwarding Policy**.

The screen displays the name of existing Bonjour forwarding policies.

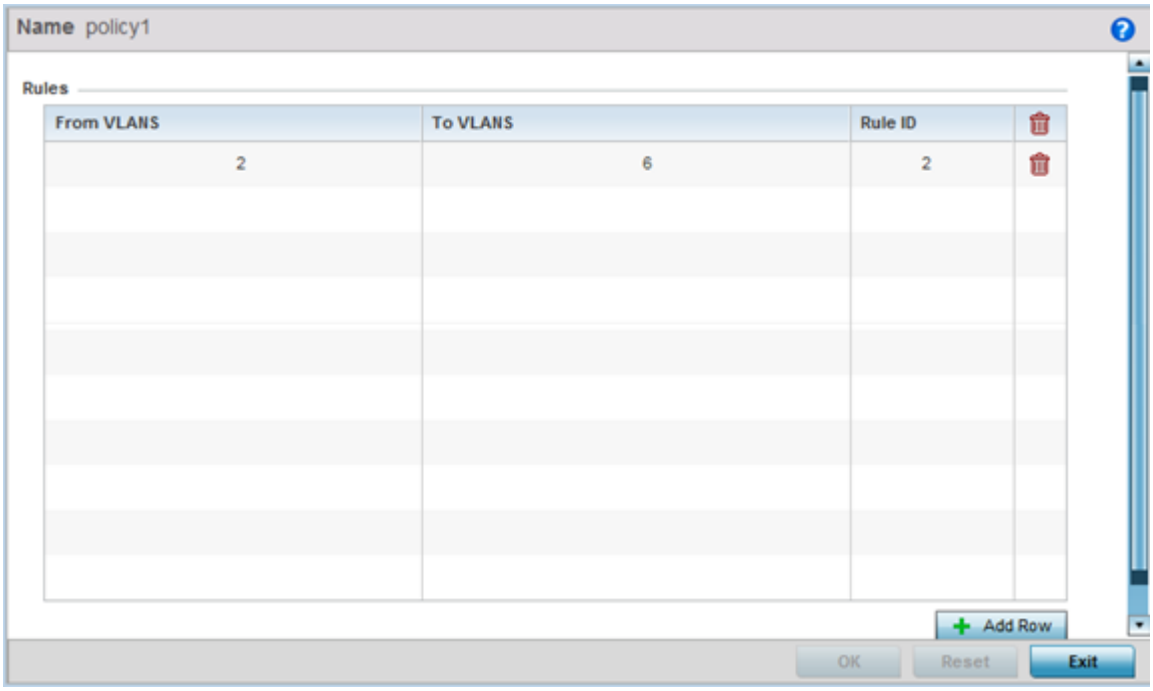



**Figure 394: Bonjour Gateway - Forwarding Policy Screen**

5 Select an existing policy and select **Edit** to modify its configuration or select **Add** to create a new configuration..

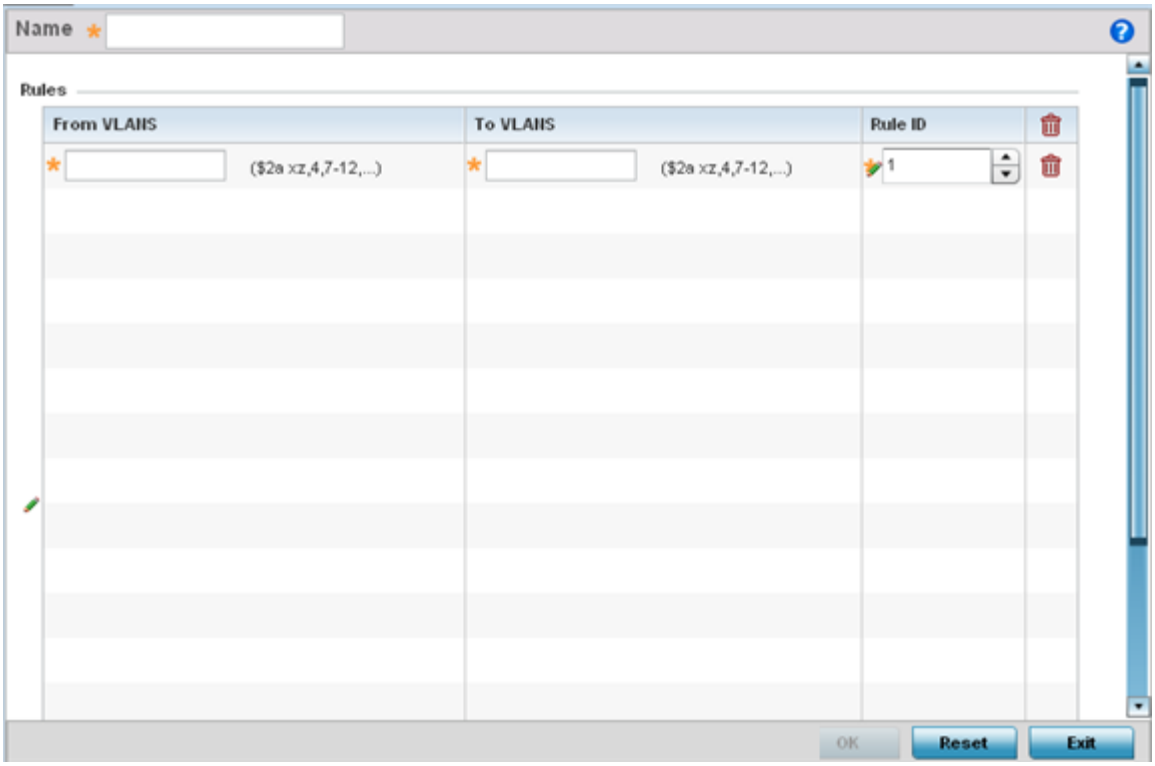



**Figure 395: Bonjour Gateway - Forwarding Policy - Add Screen**

6 Select the **+ Add Row** button to add a forwarding rule to the Bonjour Forwarding Policy.

Advertisements from VLANs that contain services are forwarded to VLANs containing clients.

| | |
|---|---|
| From VLANs | *From VLANs* are virtual interfaces where the Apple services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used. |
| To VLANs | *To VLANs* are virtual interfaces where clients for the services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used. |
| Rule ID | Use the spinner to set a unique rule ID (from 1 - 16) for this rule. This acts as numerical differentiator from other indexes. |

7 Click **OK** to save updates to this Bonjour Gateway Forwarding policy.

Click **Reset** to revert the screen to its last saved configuration.

## Setting the DHCPv6 Server Policy

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non-duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the default domain and DNS name-server address, can be passed back to the client. Address pools can be

assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

**Note**
DHCPv6 server updates are only implemented when the controller, service platform or service platform is restarted.

Refer to the following for more information on configuring the DHCPv6 Server Policy parameters:

- Defining DHCPv6 Options on page 820
- DHCPv6 Pool Configuration on page 822

To access and review the local DHCPv6 server configuration:

1 Select **Configuration** > **Services** > **DHCPv6 Server Policy**.

The DHCPv6 Server Policy screen displays.

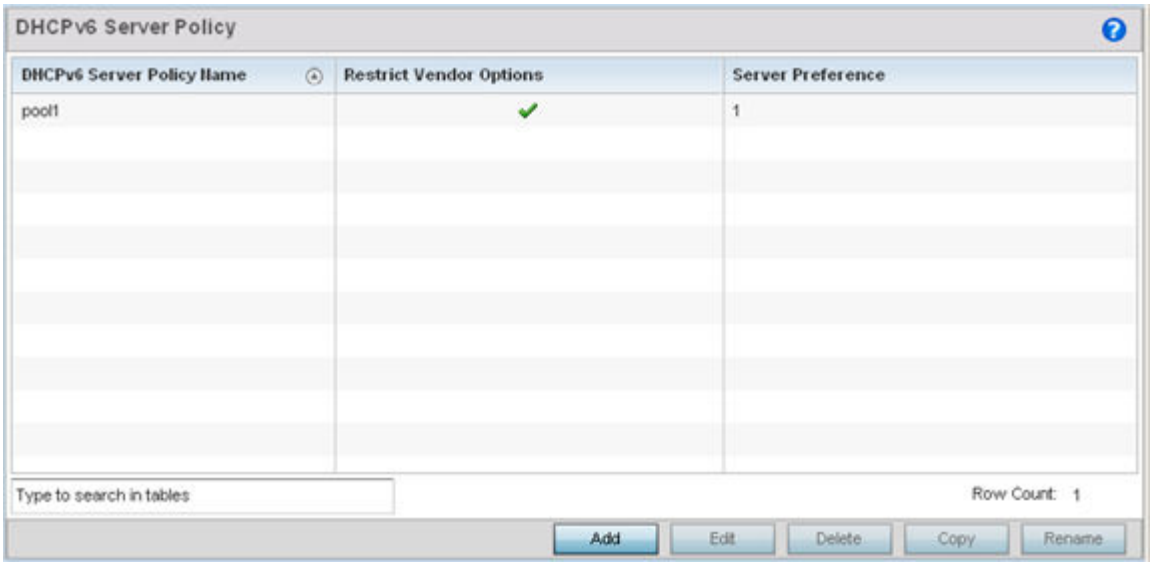



**Figure 396: DHCPv6 Server Policy Screen**

2 Review the following DHCPv6 server configurations (at a high level) to determine whether a new server policy requires creation, an existing policy requires modification or an existing policy requires deletion:

| | |
|---|---|
| DHCPv6 Server Policy Name | The name assigned to each DHCPv6 server policy when it was initially created. The name assigned to a DHCPv6 server policy cannot be modified as part of the policy edit process. However, obsolete policies can be deleted, copied (archived) or renamed as needed. |
| Restrict Vendor Options | A green checkmark within this column means this policy has been set to restrict vendor DHCP options. A red "X" defines the policy as accepting all DHCP vendor options. Vendor specific DHCPv6 options apply only to the vendor class defined. |
| Server Preferences | Lists the server preference (from 0 - 255) specified for each DHCPv6 server policy. The default value is 0. |

3 Select **Add** to create a new DHCPv6 server policy, choose an existing policy and select the **Edit** button to modify the policy's properties, or choose an existing policy and select **Delete** to remove the policy from those available.

Adding or Editing a DHCP server policy displays the DHCPv6 Server Policy Name screen by default.

## Defining DHCPv6 Options

DHCPv6 services are available for specific IP interfaces. A pool (or range) of IPv6 network addresses and DHCPv6 options can be created for each IPv6 interface defined. This range of addresses can be made available to DHCPv6 enabled devices on either a permanent or leased basis. DHCPv6 options are provided to each client with a DHCPv6 response and provide DHCPv6 clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCPv6 client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCPv6 client.

To set DHCPv6 options:

1 Select **Configuration** > **Services** > **DHCPv6 Server Policy**.

2 Select **Add** to create a new policy or **Edit** to modify the properties of a selected DHCPv6 server policy.

Select **+ Add Row** to populate the screen with editable rows for DHCPv6 option configuration.

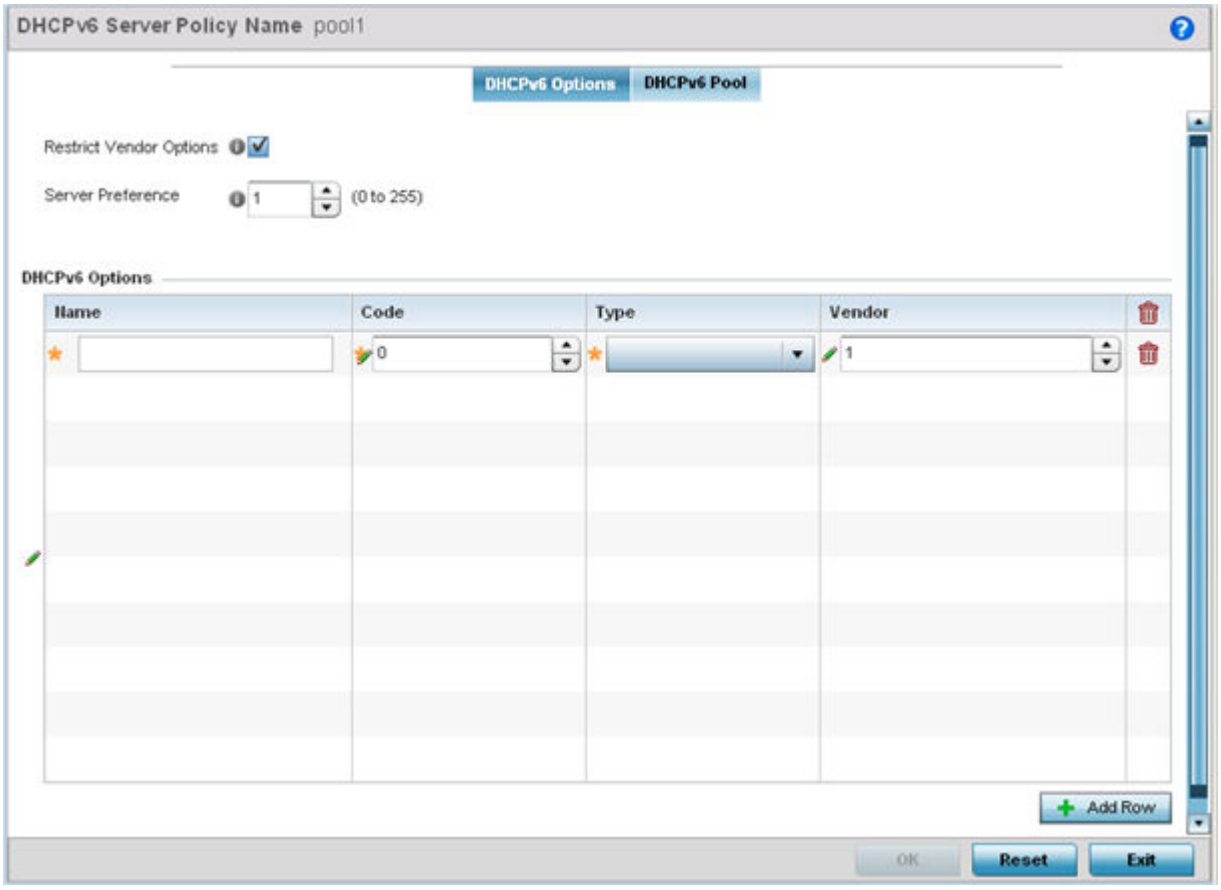



**Figure 397: DHCPv6 Server Policy - DHCPv6 Options Tab**

3 Select **Restrict Vendor Options** to restrict the use of vendor specific DHCPv6 options.

This limits the use of vendor specific DHCP options in this specific DHCPv6 policy.

4 Use the spinner control to select a **DHCPv6 Server Preference** from 0 - 255.

The default value is 0.

5 Set the following **DHCPv6 Option** configuration parameters:

| | |
|---|---|
| Name | Enter a name to associate with the new DHCP option. This name should describe the new option's function. |
| Code | Use the spinner control to specify a DHCP option code (from 0 - 254) for the option. Only one code for each DHCPv6 option of the same value can be used in each DHCPv6 server policy. |

| | |
|---|---|
| Type | Use the drop-down menu to select the DHCP option type for the new option. The option can be either ASCII, which sends an ASCII compliant string to the client, ipv6 which sends an IPv6 compatible address to the client or Hex String which sends a hexadecimal string to the client. |
| Vendor | Use the spinner control to specify the numeric Vendor ID for the new option. Each vendor should have a unique vendor ID used by the DHCPv6 server to issue vendor specific DHCP options. |

6 Click **OK** to save the updates to the DHCPv6 options.

Click **Reset** to revert the screen to its last saved configuration.

## DHCPv6 Pool Configuration

A DHCPv6 pool includes information about available configuration parameters and policies controlling the assignment of the parameters to requesting clients from the pool.

To create a DHCPv6 pool configuration:

1 Select the **DHCPv6 Pool** tab.

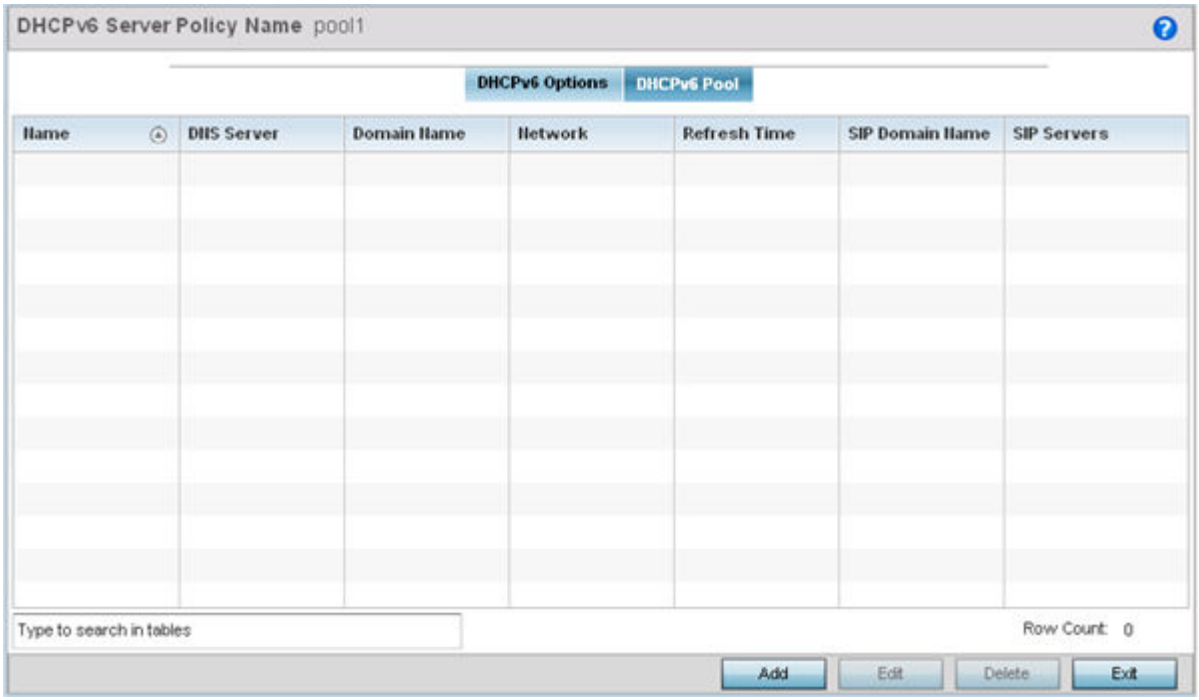



**Figure 398: DHCP Server Policy - DHCPv6 Pool Tab**

2 Refer to the following to review existing DHCPv6 Pool configuration to detremine if a new configuration is needed or an existing configuration needs to be modified or edited.

| | |
|---|---|
| Name | Lists the administrator assigned name of the IPv6 pool resource from which IPv6 formatted addresses can be issued to DHCPv6 client requests. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| DNS Server | Displays the address of the DNS server resource utilized with the DHCPv6 pool. |
| Domain Name | Displays the hostname of the domain associated with the DHCPv6 pool. |

| | |
|---|---|
| Network | Displays the IPv6 formatted address and mask utilized with the DHCPv6 address pool. The address can be configured in the Add/Edit screen. |
| Refresh Time | Displays the time, in seconds, between refreshes of the DHCPv6 address pool. |
| SIP DomainName | Displays the domain name associated with the *Session Initiation Protocol* (SIP) server that is used to prioritize voice and video traffic on a network. SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has several components (user agents, proxy servers, redirect servers, and registrars). User agents can contain SIP clients; proxy servers always contain SIP clients. |
| SIP Servers | Displays the IPv6 formatted address of the SIP server associated with the DHCP pool. |

*Adding or Editing DHCPv6 Server Configuration*

1 Select **Add** to create a new DHCPv6 pool configuration or **Edit** to modify the policy's properties of a selected DHCPv6 pool.

**Delete** obsolete policies as warranted.

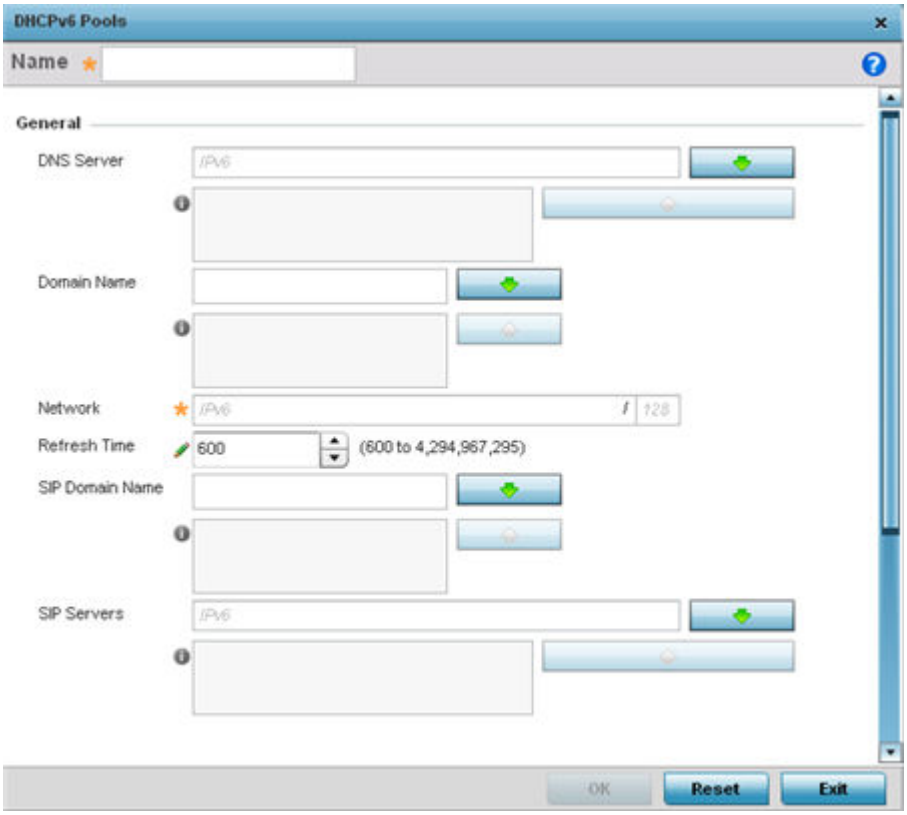



**Figure 399: DHCP Server Policy - DHCPv6 Pool - Add/Edit Screen**

2 Set the following **General** DHCPv6 pool parameters:

| | |
|---|---|
| Name | Provide as administrator assigned name for the IPv6 pool resource from which IPv6 formatted addresses can be issued to DHCPv6 client requests. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| DNS Server | Enter the IPv6 formatted address of the DNS server utilized by the DHCP pool. |

| | |
|---|---|
| Domain Name | Enter the hostname or hostnames of the domain(s) utilized with the DHCP pool. A hostname cannot contain an underscore. |
| Network | Enter the IPv6 formatted address and mask associated with the DHCPv6 pool. |
| Refresh Time | Use the spinner control to set the time, in seconds, between refreshes of the DHCPv6 address pool. The refresh time can be set from 600 - 4,294,967,295 seconds. |
| SIP DomainName | Configure the domain name or domain names associated with the Session Initiation Protocol (SIP) servers used to prioritize voice and video traffic on a network. SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has several components (user agents, proxy servers, redirect servers, and registrars). User agents can contain SIP clients; proxy servers always contain SIP clients. |
| SIP Servers | Configure the IPv6 formatted address or addresses of the SIP servers associated with the DHCP pool. |

3 If you are using DHCPv6 options in the pool, set the following within the **DHCPv6 Options Value** table.

| | |
|---|---|
| Name | Use the drop-down menu to select an existing DHCP option name from the existing options configured in DHCPv6 Options. If no suitable option is available click the create button to define a new option. |
| Value | Enter or modify the numeric ID setting for the selected DHCP option. |

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

Click **Reset** to revert to the last saved configuration.

## Setting the RADIUS Configuration

*Remote Authentication Dial-In User Service* (RADIUS) is a client/server protocol and software enabling remote access servers to authenticate users and authorize their access. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the controller, service platform or access point's local RADIUS server containing user authentication and network service access information.

RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to the controller, service platform or access point, authentication requests are sent to the RADIUS server. Authentication and encryption takes place through the use of a shared secret password (not transmitted over the network).

The local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assign policies for the group authorization.

The access point allows the enforcement of user-based policies. User policies include dynamic VLAN assignment and access based on time of day. The access point uses a default trustpoint. A certificate is required for EAP TTLS,PEAP and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after authentication with the RADIUS server. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

To view RADIUS configurations:

1 Select the **Configuration** tab from the main menu.
2 Select the **Services** tab.

The upper, left-hand side pane of the user interface displays the **RADIUS** option. The RADIUS Group screen displays by default.

For information on creating the groups, user pools and server policies needed to validate user credentials against a server policy configuration, refer to the following:

- Creating RADIUS Groups on page 825
- Defining User Pools on page 828
- Configuring RADIUS Server Policy on page 833

## Creating RADIUS Groups

The RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in a local database. The user ID in the received access request is mapped to the specified group for authentication. RADIUS groups allows the enforcement of the following policies managing user access.

- Assign a VLAN to the user upon successful authentication
- Define a start and end of time in (HH:MM) when the user is allowed to authenticate
- Define the list of SSIDs to which a user belonging to this group is allowed to associate
- Define the days of the week the user is allowed to login
- Rate limit traffic

To access the RADIUS Groups menu:

1 Select **Configuration** > **Services** > **RADIUS** from the main menu.
2 Select **Groups**.

The browser displays a list of the existing groups.

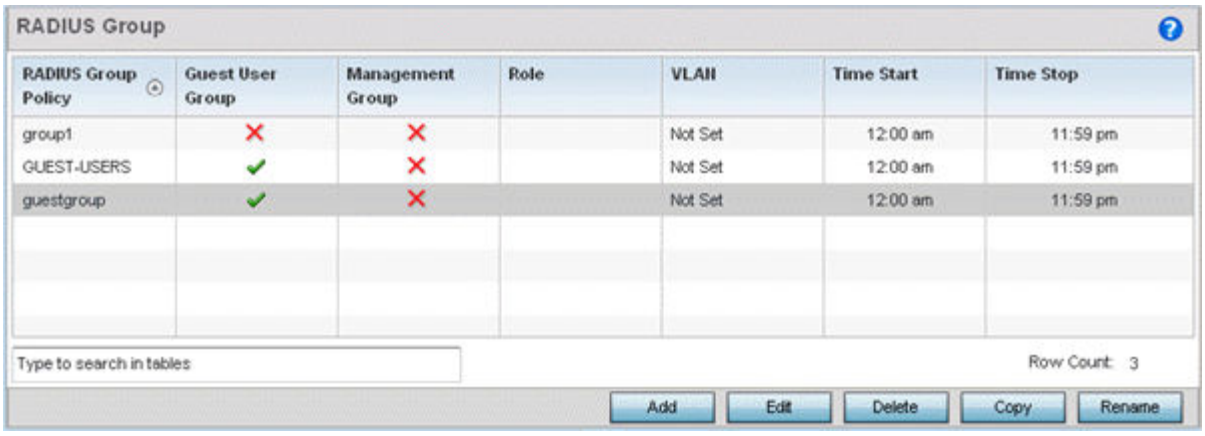



**Figure 400: RADIUS Group Screen**

3 Select a group from the Group Browser to view the following read-only information for existing groups:

| | |
|---|---|
| RADIUS Group Policy | Displays the group name or identifier assigned to each listed group when it was created. The name cannot exceed 32 characters or be modified as part of the group edit process. |
| Guest User Group | Specifies whether a user group only has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each group. A red "X" designates the group as having permanent access to the local RADIUS server. Guest user groups cannot be made management groups with unique access and role permissions. |
| Management Group | A green checkmark designates this RADIUS user group as a management group. Management groups can be assigned unique access and role permissions. |
| Role | If a group is listed as a management group, it may also have a unique role assigned. Available roles include:<br>• **monitor** - Read-only access<br>• **helpdesk** - Helpdesk/support access<br>• **network-admin** - Wired and wireless access<br>• **security-admin** - Full read/write access<br>• **system-admin** - System administrator access<br>• **superuser** - Super user access<br>• **webuser-admin** - Rights to manage captive portal users<br>• **vendor-admin** - Rights to manage device onboarding |
| VLAN | Displays the group's VLAN ID. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the network (once authenticated by the local RADIUS server). |
| Time Start | Specifies the time users within each listed group can access local RADIUS resources. |
| Time Stop | Specifies the time users within each listed group lose access to local RADIUS resources. |

4 Click **Add** to create a new RADIUS group, **Edit** to modify the configuration of an existing group, or **Delete** to permanently remove a selected group.

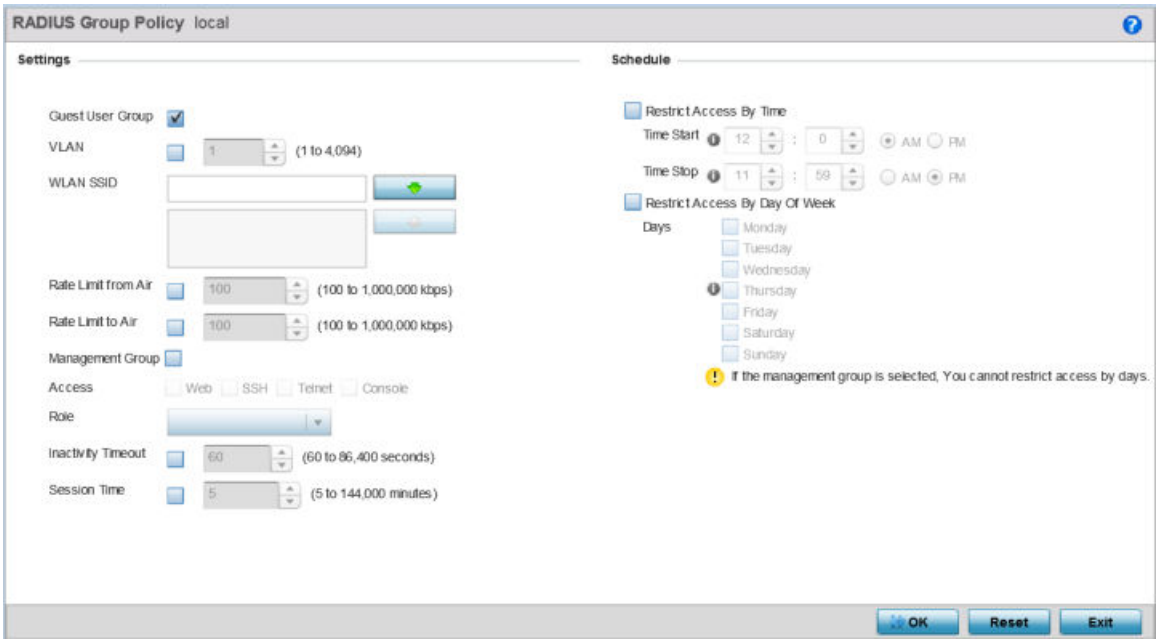



**Figure 401: RADIUS Group Policy - Add/Edit Screen**

5 Define the following settings to define the user group configuration:

| | |
|---|---|
| RADIUS Group Policy | If you are creating a new RADIUS group, assign it a name to help differentiate it from others with similar configurations. The name cannot exceed 32 characters or be modified as part of a RADIUS group edit process. |
| Guest User Group | Select this option to assign only guest access and temporary permissions to the local RADIUS server. Guest user groups cannot be made management groups with unique access and role permissions. |
| VLAN | Select this option to assign a specific VLAN to this RADIUS user group. Ensure Dynamic VLAN assignment (single VLAN) is enabled for the WLAN in order for the VLAN assignment to work properly.<br>For more information, see “Configuring WLAN Basic Configuration” on page 529. |
| WLAN SSID | Assign a list of SSIDs users within this RADIUS group are allowed to associate with. An SSID cannot exceed 32 characters. Assign WLAN SSIDs representative of the configurations a guest user will need to access. The parameter is not available if this RADIUS group is a management group. |
| Rate Limit from Air | Select the checkbox to set the rate limit for clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Setting a value of 0 disables rate limiting. |
| Rate Limit To Air | Select the checkbox to set the rate limit from clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Setting a value of 0 disables rate limiting. |
| Management Group | Select this option to designate this RADIUS group as a management group. If set as management group, assign member roles (System-Admin, Help Desk etc.) using the **Role** drop-down menu. This feature is disabled by default. |

| | |
|---|---|
| Access | If a group is listed as a management group, assign how the devices can be accessed. Available access types are:<br>• **Web** - Web access through browser is permitted.<br>• **SSH** - SSH access through command line is permitted.<br>• **Telnet** - Telnet access through command line is permitted.<br>• **Console** - Console access to the device is permitted. |
| Role | If a group is listed as a management group, it may also have a unique role assigned. Available roles include:<br>• **monitor** - Read-only access<br>• **helpdesk** - Helpdesk/support access<br>• **network-admin** - Wired and wireless access<br>• **security-admin** - Full read/write access<br>• **system-admin** - System administrator access<br>• **superuser** - Super user access<br>• **webuser-admin** - Rights to manage captive portal users<br>• **vendor-admin** - Rights to manage device onboarding |
| Inactivity Timeout | ESelect the option to enable inactivity timeout. Use the drop-down menu to specify an interval in Seconds (60 - 86,400). When, for this duration no frame is received, the session is timed out.<br>The default is 60 seconds. |
| Session Time | Select the option to enable session timeout. Use the drop-down menu to set a client session time in Minutes (5 - 144,000). This is the session time a client is granted upon successful authentication. When this time expires, the RADIUS session is terminated. |

6 Set the **Schedule** to configure access times and dates.

Select **Restrict Access By Time** to enable time-based access.

| | |
|---|---|
| Time Start | Use the spinner control to set the time (in HH:MM format) RADIUS group members are allowed access the RADIUS server resources. Select either the **AM** or **PM** radio button to set the time as morning or evening. |
| Time Stop | Use the spinner control to set the time (in HH:MM format) RADIUS group members are denied access to RADIUS server resources. Select either the **AM** or **PM** radio button to set the time as morning or evening. If already logged in, the RADIUS group user is deauthenticated from the WLAN. |
| Days | Optionally select the **Restrict Access by Day Of Week** option, and select the days on which RADIUS group members can access RADIUS resources. This is an additional means of refining the access permissions of RADIUS group members. |

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

Click **Reset** to revert to the last saved configuration.

## Defining User Pools

A user pool defines policies for individual user access to local (controller, service platform or Access Point managed) RADIUS resources. User pools are a convenient means of providing RADIUS resources based on the pool's unique permissions (temporary or permanent). A pool can contain a single user or group of users.

To configure a RADIUS user pool and unique user IDs:

1 Select **Configuration** → **Services** → **RADIUS** from the main menu.

2 Select **User Pools**.

The RADIUS User Pool screen lists the default pool along with any other admin created user pool.

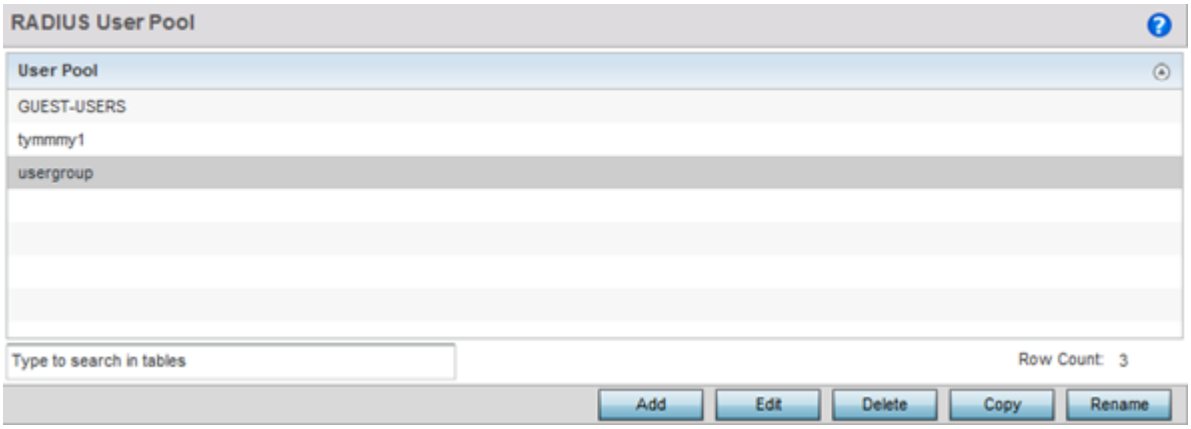



**Figure 402: RADIUS User Pool Screen**

3 Click **Add** to create a new RADIUS user pool, **Edit** to modify the configuration of an existing pool, or **Delete** to permanently remove a selected pool.

4 If you are creating a new pool, assign it a name up to 32 characters and click **Continue**.

The name should be representative of the users comprising the pool and/or the temporary or permanent access privileges assigned.

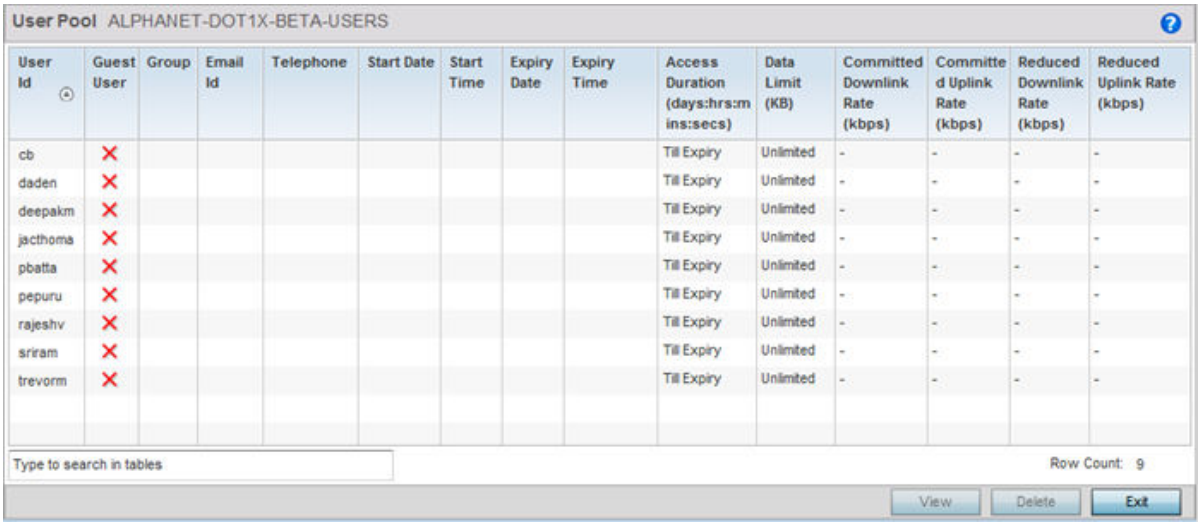



**Figure 403: RADIUS User Pool - User Pools - Details Screen**

5 Refer to the following **User Pool** configurations.

They define when specific user IDs have access to the access point's RADIUS resources.

| | |
|---|---|
| User ID | The unique string identifying this user. This is the ID assigned to the user when created and cannot be modified with the rest of the configuration. |
| Guest User | Specifies (with a green check) the user has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each user. A red “X” designates the user as having permanent access to the local RADIUS server. |
| Group | The group name each configured user ID is a member. |
| Email ID | The configured E-mail ID for this user. This is the address used when communicating with users in this pool. |
| Telephone | The configured telephone number for this user. This is the number used when communicating with users in this pool. |
| Start Date | The month, day and year the listed user ID can access the access point’s internal RADIUS server resources. |
| Start Time | The time the listed user ID can access the internal RADIUS server. The time applies only to the range defined by the start and expiry date. |
| Expiry Date | The month, day and year the listed user ID can no longer access the internal RADIUS server. |
| Expiry Time | The time the listed user loses access to internal RADIUS server resources. The time applies only to the range defined by the start and expiry date. |
| Access Duration (days:hrs:mins:secs) | The amount of time a user is allowed access when time-based access privileges are applied. The duration cannot exceed 365 days. |
| Data Limit (KB) | The total amount of bandwidth (in kilobytes) consumable by each guest user. |
| Committed Downlink Rate (kbps) | The download speed (in kilobytes) allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the **Reduced Downlink Rate**. |
| Committed Uplink Rate (kbps) | The upload speed (in kilobytes) allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the **Reduced Uplink Rate**. |
| Reduced Downlink Rate (kbps) | The reduced speed the guest utilizes (in kilobytes) when exceeding their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the **Reduced Downlink Rate**. |
| Reduced Uplink Rate (kbps) | The reduced speed the guest utilizes (in kilobytes) when exceeding their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the **Reduced Uplink Rate**. |

6 Click **Add** to add a new RADIUS user, **Edit** to modify the configuration of an existing user or **Delete** to remove an existing user ID.

Select a RADIUS user and click **Copy** to make a copy of the user to make further modifications or use **Rename** to rename the existing RADIUS user.

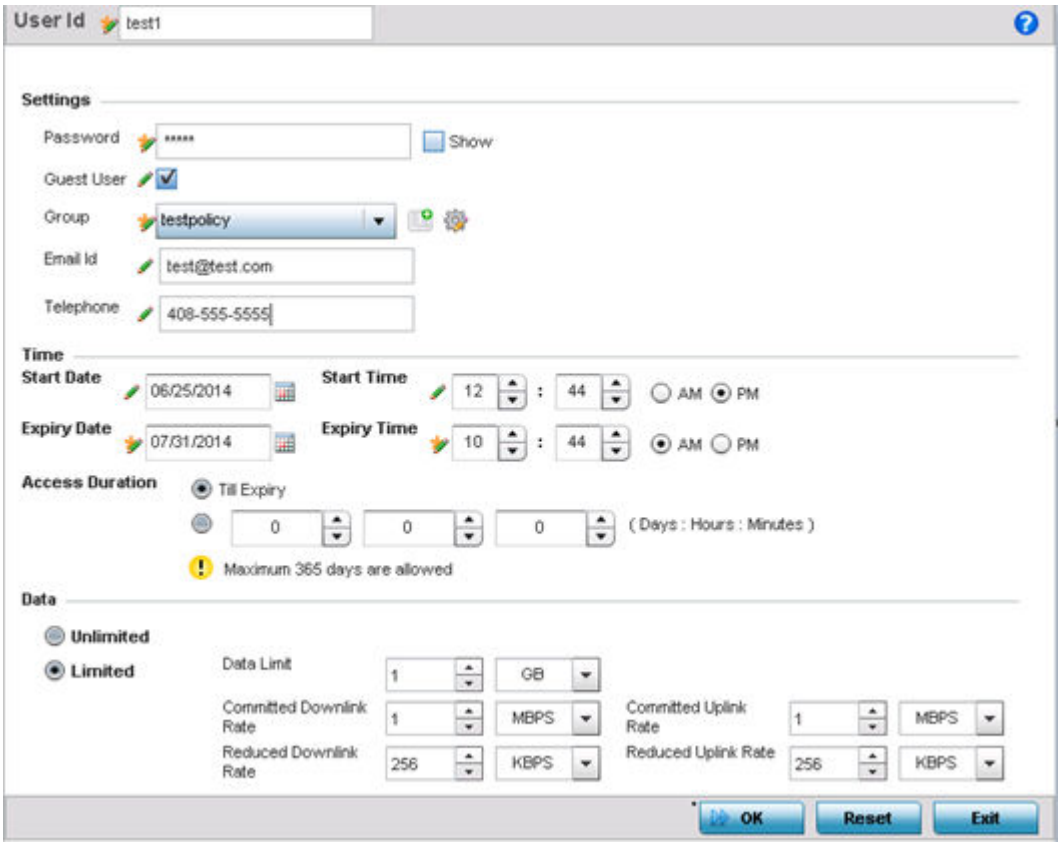



**Figure 404: RADIUS User Pool - Add/Edit - Users Screen**

7 Refer to the following settings to create a new user with unique access privileges:

| | |
|---|---|
| User ID | Assign a unique character string identifying this user. The ID cannot exceed 64 characters. |
| Password | Provide a password unique to this user ID. The password cannot exceed 32 characters. Select the **Show** checkbox to expose the password's actual character string. Otherwise the password displays as a string of asterisks (*). |
| Guest User | Select the check box to designate this user as a guest with temporary access. The guest user must be assigned unique access times to restrict their access. |
| Group | If the user has been defined as a guest, use the **Group** drop-down menu to assign the user a group with temporary access privileges. If the user is defined as a permanent user, select a group from the group list. If no groups are relevant to the user's intended access, select the **Create** link (or icon for guests) and create a new group configuration suitable for the user's membership.<br>For more information, see Creating RADIUS Groups on page 825. |

| | |
|---|---|
| Email ID | Set the email ID for this user. |
| Telephone | Specify the telephone number for this user.<br>Specify the 12-character maximum telephone number of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool. |

8 Refer to the following **Time** settings to define time-based guest user access privileges:

| | |
|---|---|
| Start Date | Enter a start date, or use the calendar icon to select a starting date for the user's credentials to start working. |
| Start Time | Enter a start time, or use the spinner controls to select a starting time for the user's credentials to start working. Use the **AM** and **PM** buttons to apply a morning or afternoon/evening designation. |
| Expiry Date | Enter an end date, or use the calendar icon to define an expiration date for the user's credentials. Selecting this option enables the **Till Expiry** radio button. |
| Expiry Time | If you are using the **Till Expiry** option, enter an end time, or use the spinner controls to select an ending time for the user's credentials to expire. Use the **AM** and **PM** buttons to apply a morning or afternoon/evening designation. |
| Access Duration | Specify the time a user can access the system when time based access privilege are applied. Select **Till Expiry** to allow user access until their configured expiry date and time are met. To limit the time a user can access the captive portal during their configured time period, specify the Days, Minutes, and Seconds the user is allowed access. The Access Duration cannot exceed 365 days. |

9 To allow the guest user unlimited data usage, select **Unlimited**.

To limit bandwidth, select **Limited** and refer to the **Data** field to create bandwidth based access privileges:

| | |
|---|---|
| Data Limit | Use the spinner control to specify the maximum bandwidth consumable by the guest user. Once a value is configured, select the measurement as either GB (gigabytes) or MB (megabytes). |
| Committed Downlink Rate | Use the spinner control to specify the download speed dedicated to the guest user. When bandwidth is available, the user can download data at the specified rate. Once a value is configured, select the measurement as either MBPS (Megabytes per second) or KBPS (Kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the defined **Reduced Downlink Rate**. |
| Reduced Downlink Rate | Use the spinner control to specify a reduced speed for guest operation when they have exceeded their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the **Reduced Downlink Rate**. Once a value is configured, select the measurement as either MBPS (Megabytes per second) or KBPS (Kilobytes per second). |
| Committed Uplink Rate | Use the spinner control to specify the upload speed dedicated to the guest user. When bandwidth is available, the user is able to upload data at the specified rate. Once a value is configured, select the measurement as either MBPS (Megabytes per second) or KBPS (Kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the **Reduced Uplink Rate**. |
| Reduced Uplink Rate | Use the spinner control to specify a reduced speed for guest operation when they've exceed their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the **Reduced Uplink Rate**. Once a value is configured, select the measurement as either MBPS (Megabytes per second) or KBPS (Kilobytes per second). |

10 Click **OK** to save the user's group membership configuration.

Click **Reset** to revert to the last saved configuration.

## Configuring RADIUS Server Policy

A RADIUS server policy is a unique authentication and authorization configuration for receiving user connection requests, authenticating users, and returning the configuration information necessary for the RADIUS client to deliver service to the user. An access point's requesting client is the entity with authentication information requiring validation. The access point's local RADIUS server has access to a database of authentication information used to validate client authentication requests.

The RADIUS server ensures the information is correct using an authentication scheme like *PAP*, *CHAP* or *EAP*. The user's proof of identification is verified, along with, optionally, other information. A RADIUS server policy can also use an external LDAP resource to verify user credentials. The creation and utilization of a single RADIUS server policy is supported.

To manage the access point's RADIUS server policy:

1 Select **Configuration** → **Services** from the main menu.

2 Expand the **RADIUS** menu option and select **RADIUS Server**.

The RADIUS Server Policy screen displays with the Server Policy tab displayed by default.

s

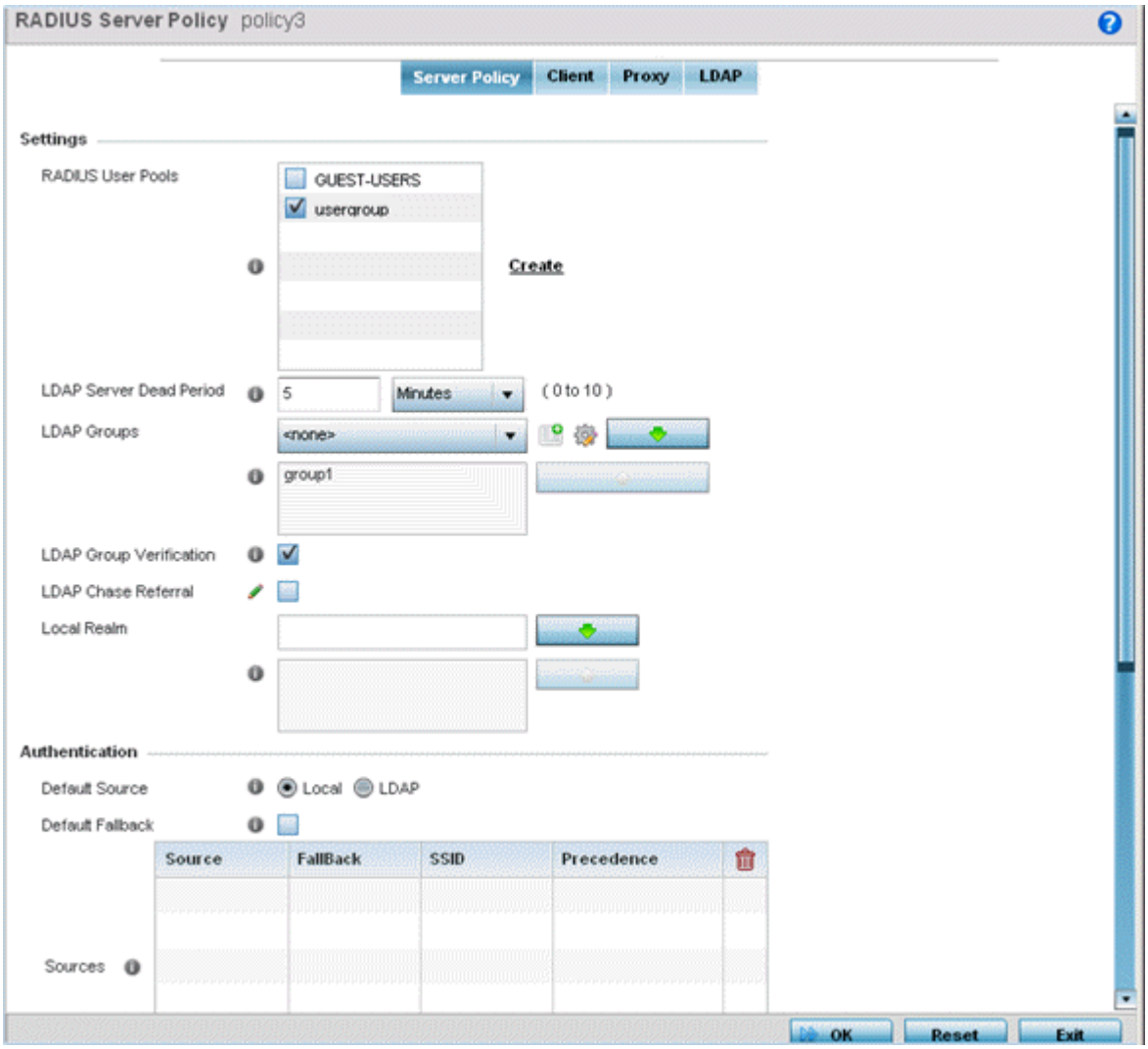



**Figure 405: RADIUS Server Policy Screen - Server Policy Tab**

3 Select **Activate RADIUS Server Policy** to enable the parameters within the screen for configuration.

Ensure that thiis option remains selected, or this RADIUS server configuration will not be applied to the access point profile.

4 Define the following settings required to create or modify the server policy.

| | |
|---|---|
| RADIUS Server Policy | Select the user pools (groups of existing client users) to apply to this server policy. If there is not an existing user pool configuration suitable for the deployment, select the **Create** link and define a new configuration. For more information, see Defining User Pools on page 828. |
| LDAP Server Dead Period | Set an interval in either seconds (0 - 600) or minutes (0- 10) during which the access point will not contact its LDAP server resource. A dead period is only implemented when additional LDAP servers are configured and available. |

| | |
|---|---|
| LDAP Groups | Use the drop-down menu to select LDAP groups to apply the server policy configuration. Select the Create or Edit icons as needed to either create a new group or modify an existing group. Use the arrow icons to add and remove groups as required. |
| LDAP Group Verification | Select the check box to set the LDAP group search configuration. This setting is enabled by default. |
| LDAP Chase Referral | Select the check box to set the LDAP referral chase feature. This settings is enabled by default. When enabled, if the LDAP server does not contain the requested information, it indicates to the LDAP client that it does not have the requested information and provides the client with another LDAP server that could have the requested information. It is up to the client to contact the other LDAP server for its information. |
| Local Realm | Define the LDAP Realm performing authentication using information from an LDAP server. User information includes user name, password, and the groups to which the user belongs. |

5 Set the following **Authentication** parameters to define server policy authorization settings.

| | |
|---|---|
| Default Source | Select the RADIUS resource for user authentication with this server policy. Options include **`Local`** for the local user database or **`LDAP`** for a remote LDAP resource. The default setting is **`Local`**. |
| Default Fallback | Select this option to indicate that fall back from RADIUS to local is enabled in case RADIUS authentication is not available for any reason. This option is enabled only when LDAP is selected as the Default Source. Use the **Add Row** button to add fallback sources into the **Sources** table. Provide the following information:<br>• Source – Select the type of fallback. Select from **`LDAP`** or **`Local`**.<br>• Fallback – Select to enable fallback on this record.<br>• SSID – Enter the SSID to fall back on.<br>• Precedence – Use the spinner to select the precedence for selection of fallback. |
| Authentication Type | Use the drop-down menu to select the EAP authentication scheme used with this policy. The following EAP authentication types are supported:<br>• All – Enables both TTLS and PEAP<br>• TLS - Uses TLS as the EAP type<br>• TTLS and MD5 - The EAP type is TTLS with default authentication using MD5<br>• TTLS and PAP - The EAP type is TTLS with default authentication using PAP<br>• TTLS and MSCHAPv2 - The EAP type is TTLS with default authentication using MSCHAPv2<br>• PEAP and GTC - The EAP type is PEAP with default authentication using GTC<br>• PEAP and MSCHAPv2 - The EAP type is PEAP with default authentication using MSCHAPv2<br><br>However, when user credentials are stored on an LDAP server, the RADIUS server cannot conduct PEAP-MSCHAPv2 authentication on its own, as it is not aware of the password. Use LDAP agent settings to locally authenticate the user. Additionally, an authentication utility (such as Samba) must be used to authenticate the user. Samba is an open source software used to share services between Windows and Linux machine. |
| Do Not Verify Username | Enabled only when **`TLS`** is selected in **Authentication Type**. When selected, user name is not matched but the certificate expiry is checked. |

| | |
|---|---|
| Enable CRL Validation | Select this option to enable a *Certificate Revocation List* (CRL) check. Certificates can be checked and revoked for a number of reasons including failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. This option is disabled by default. |
| Enable EAP Termination | Select this option to enable EAP Termination on the current RADIUS server policy. EAP Termination terminates EAP authentication at the controller |
| Bypass CRL Check | Select the option to bypass a *certificate revocation list* (CRL) check when a CRL is not detected. This setting is enabled by default. A CRL is a list of certificates that have been revoked or are no longer valid. |
| Allow Expired CRL | Select this option to allow the use of an expired CRL. This option is enabled by default |

Note

When you are using LDAP as authentication external source, the PEAP-MSCHAPV2 authentication type can be used only if the LDAP server returns the password as plain-text. PEAP-MSCHAPv2 authentication is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory Server.

6 If you are using LDAP as the default authentication source, select **+ Add Row** to set LDAP Agent settings.

When a user's credentials are stored on an external LDAP server, the controller or service platform's local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource using credentials maintained locally.

| | |
|---|---|
| Username | Enter a 128-character maximum username for the LDAP server's domain administrator. This is the username defined on the LDAP server for RADIUS authentication requests. |
| Password | Enter and confirm the 32-character maximum password (for the username provided above). The successful verification of the password maintained on the controller or service platform enables PEAP-MSCHAPv2 authentication using the remote LDAP server resource. |
| Retry Timeout | Set the number of seconds (60 - 300) or minutes (1 - 5) to wait between LDAP server access requests when attempting to join the remote LDAP server's domain. The default setting is one minute. |
| Redundancy | Define the Primary or Secondary LDAP agent configuration used to connect to the LDAP server domain. |
| Domain Name | Enter the name of the domain (from 1 - 127 characters) to which the remote LDAP server resource belongs. |

7 Set the following **Session Resumption/Fast Reauthentication** settings to define how server policy sessions are re-established once terminated and require cached data to resume:

| | |
|---|---|
| Enable Session Resumption | Select the checkbox to control volume and the duration cached data is maintained by the server policy upon the termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption. This setting is disabled by default. |
| Cached Entry Lifetime | If enabling session resumption, use the spinner control to set the lifetime (1 - 24 hours) cached data is maintained by the RADIUS server policy. The default setting is 1 hour. |
| Maximum Cache Entries | If enabling session resumption, use the spinner control to define the maximum number of entries maintained in cache for this RADIUS server policy. The default setting is 128 entries. |

8 Click **OK** to save the settings to the server policy configuration.

Click **Reset** to revert to the last saved configuration.

*Configuring RADIUS Server Clients*

1 Select the **Client** tab, and ensure the **Activate RADIUS Server Policy** button remains selected.

The access point uses a RADIUS client as a mechanism to communicate with a central server to authenticate users and authorize access.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash to create a 16 octet value used with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS access request packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified access accept packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified access reject message, the username and password are considered incorrect, and the user is not authenticated.

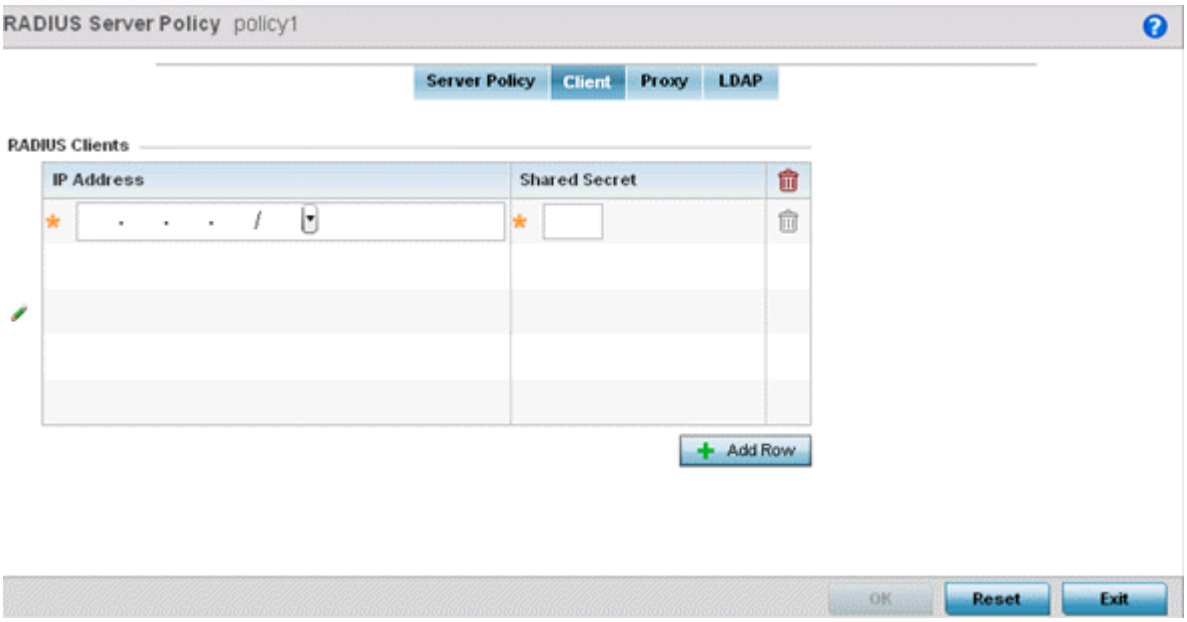



**Figure 406: RADIUS Server Policy Screen - Add/Edit - Client Tab**

2 Select the **+ Add Row** button to add a table entry for a new client's IP address, mask and shared secret.

To delete a client entry, select the Delete icon on the right-hand side of the table entry.

3 Specify the **IP Address** and mask of the RADIUS client authenticating with the RADIUS server.

4 Specify a **Shared Secret** for authenticating the RADIUS client.

Shared secrets verify RADIUS messages with a RADIUS-enabled device configured with the same shared secret. Select the **Show** checkbox to expose the shared secret's actual character string. Otherwise, the shared secret is displayed as a string of asterisks (*).

5 Click **OK** to save the server policy's client configuration.

Click **Reset** to revert to the last saved configuration.

*Configuring RADIUS Server Proxy Settings*

1 Select the **Proxy** tab, and ensure the **Activate RADIUS Server Policy** button remains selected.

A user's access request is sent to a proxy server if it cannot be authenticated by local RADIUS resources. The proxy server checks the information in the user access request, and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to the NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the access point's RADIUS server receives a request for a user name containing a realm, the server references a table of configured realms. If the realm is known, the server proxies the request to the RADIUS server. The behavior of the proxying server is configuration-dependent on most servers. In addition, the proxying server can be configured to add, remove or rewrite requests when they are proxied.

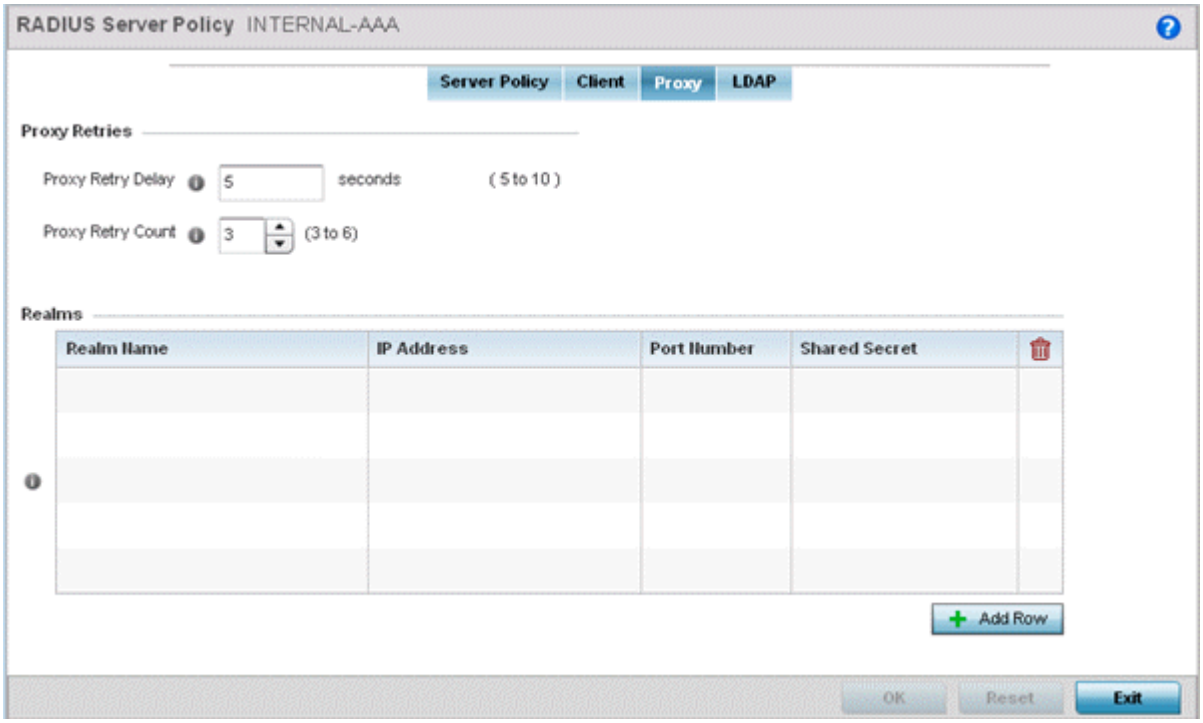



**Figure 407: RADIUS Server Policy Screen - Add/Edit - Proxy Tab**

2 Enter the **Proxy Retry Delay** as a value from 5 -10 seconds.

This is the interval the RADIUS server waits before making an additional connection attempt. The default delay interval is 5 seconds.

3 Enter the **Proxy Retry Count** as a value from 3 - 6.

This is the number of retries sent to the proxy server before giving up the request. The default retry count is 3 attempts.

4 Select the **+ Add Row** button to add a RADIUS server proxy realm name and network address.

To delete a proxy server entry, select the **Delete** icon on the right-hand side of the table.

5 Enter the realm name in the **Realm Name** field.

The realm name cannot exceed 50 characters. When the access point's RADIUS server receives a request for a user name, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

6 Enter the proxy server IP address in the **IP Address** field.

This is the address of server checking the information in the user access request. The proxy server either accepts or rejects the request on behalf of the RADIUS server.

7 Enter the TCP/IP **Port Number** for the server used as a data source for the proxy server.

Use the spinner to select a value from 1024 - 65535. The default port is 1812.

8 Enter the RADIUS client's **Shared Secret** for authenticating the RADIUS proxy.

Select the **Show** checkbox to expose the shared secret's actual character string. Otherwise, the shared secret is displayed as a string of asterisks (*).

9 Click **OK** to save the configuration.

Click **Reset** to revert to the last saved configuration.

*Configuring RADIUS Server LDAP Settings*

1 Select the **LDAP** tab, and ensure the **Activate RADIUS Server Policy** button remains selected.

Administrators have the option of using the access point's RADIUS server to authenticate users against an external LDAP server resource. An external LDAP user database allows the centralization of user information and reduces administrative user management overhead. Thus, making the RADIUS authorization process more secure and efficient.

RADIUS is not just a database. It is a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location. It is the access point's RADIUS resources that provide the tools to perform user authentication and authorize users based on complex checks and logic. There is no way to perform such complex authorization checks from a LDAP user database alone.

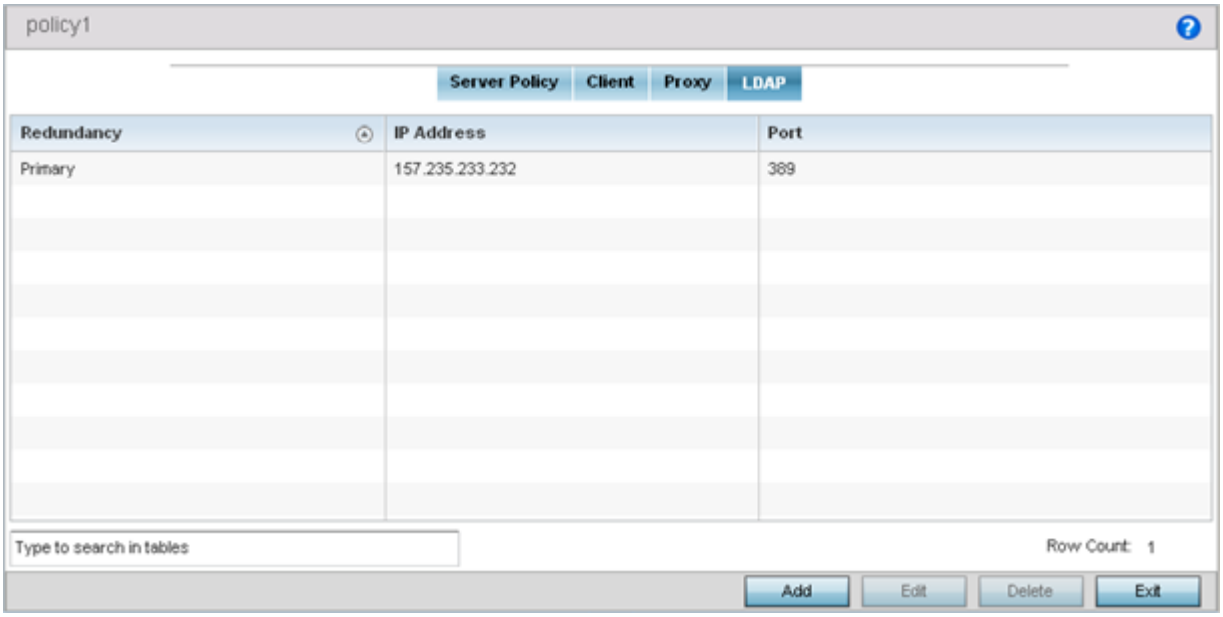



**Figure 408: RADIUS Server Policy Screen - LDAP Tab**

2 Refer to the following to determine whether an LDAP server can be used as is, a server configuration requires creation or modification, or a configuration requires deletion and permanent removal.

| | |
|---|---|
| Redundancy | Whether the listed LDAP server IP address has been defined as a *primary* or *secondary* server resource. Designating at least one secondary server is a good practice to ensure RADIUS resources are available if a primary server becomes unavailable. |
| IP Address | The IP address of the external LDAP server acting as the data source for the RADIUS server. |
| Port | The physical port number used by the RADIUS server to secure a connection with the remote LDAP server resource. |
| Timeout | The number of seconds (1- 10) this server session waits for a connection before aborting the connection attempt with the listed RADIUS server resource. |

3 Click **Add** to add a new LDAP server configuration, **Edit** to modify an existing LDAP server configuration, or **Delete** to remove a LDAP server from the list of those available.

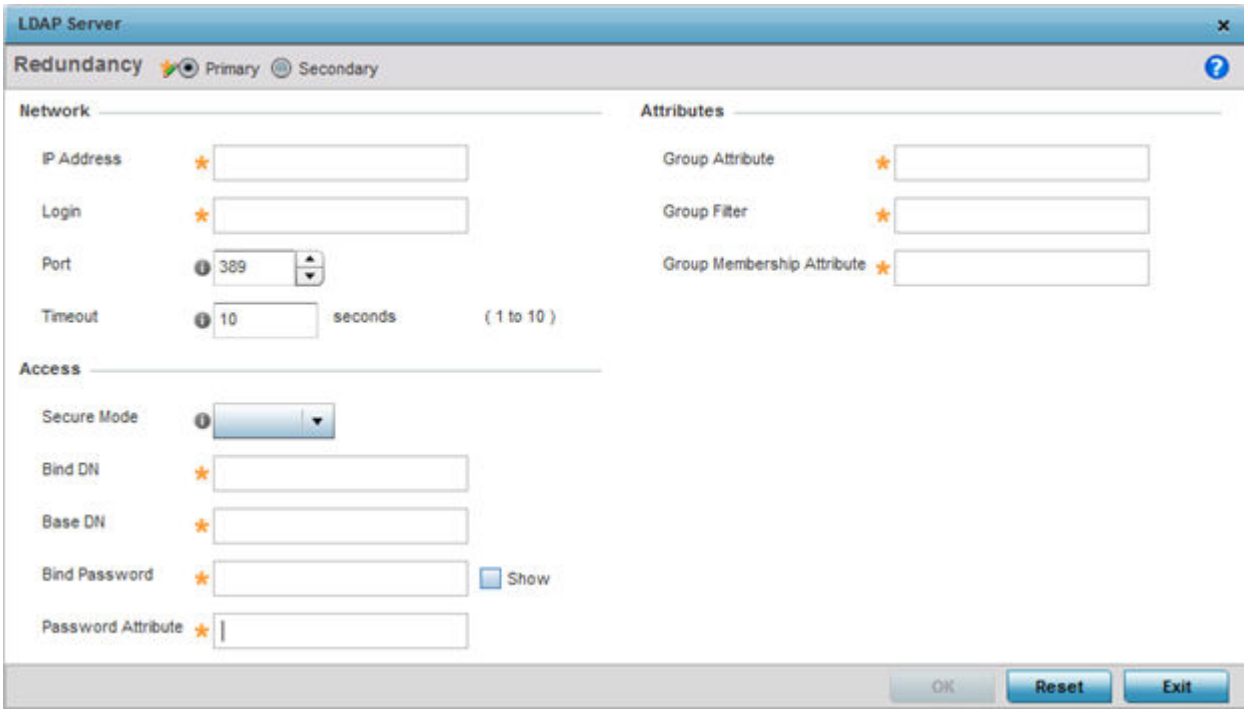



**Figure 409: LDAP Server Add Screen**

4 Set the following **Network** address information required for the connection to an external LDAP server resource:

| | |
|---|---|
| Redundancy | Whether this LDAP server is a primary or secondary server resource. Primary servers are always queried for connection first. However, designating at least one secondary server is a good practice to ensure RADIUS user information is available if a primary server becomes unavailable. |
| IP Address | The 128-character maximum IP address or FQDN of the external LDAP server acting as the data source for the RADIUS server. |
| Login | A unique login name used for accessing the remote LDAP server resource. Consider using a unique login name for each LDAP server provided to increase the security of the connection to the remote LDAP server. |
| Port | Use the spinner control to set the physical port number used by the RADIUS server to secure a connection with the remote LDAP server resource. The default port is 389.. |
| Timeout | An interval between 1 - 10 seconds the RADIUS server uses as a wait period for a response from the target primary or secondary LDAP server resource. The default setting is 10 seconds. |

5 Set the following **Access** address information required for the connection to the external LDAP server resource:

| | |
|---|---|
| Secure Mode | The security mode when connecting to an external LDAP server. Use **`start-tls`** or **`tls-mode`** to connect. The **`start-tls`** mode provides a way to upgrade a plain text connection to an encrypted connection using TLS. |
| Bind DN | The distinguished name to bind with the LDAP server. The DN is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas. |
| Base DN | A distinguished name (DN) that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with the most specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the Relative Distinguished Name (RDN). The RDN identifies an entry distinctly from any other entries that have the same parent. |
| Bind Password | A valid password for the LDAP server. Select the **Show** check box to expose the password's actual character string. Otherwise the password is displayed as a string of asterisks (*). The password cannot 32 characters. |
| Password Attribute | The LDAP server password attribute. The password cannot exceed 64 characters. |

6 Set the following **Attributes** for LDAP groups to optimally refine group queries:

| | |
|---|---|
| GroupAttribute | LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group, an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password, or group membership name. |
| Group Filter | Specify the group filters used by the LDAP server. This filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service. |
| Group Membership Attribute | Specify the group member attribute sent to the LDAP server when authenticating users. |

7 Click **OK** to save the changes to the LDAP server configuration.

Click **Reset** to revert to the last saved configuration.

## Setting the URL List

URL lists are used to select highly utilized URLs for smart caching. The selected URLs are monitored and routed according to existing cache content policies.

To configure a URL lists policy:

1 Select the **Configuration** tab from the main menu.
2 Select the **Services** tab from the Configuration menu.
3 Select **URL Lists**.

The URL Lists screen displays existing policies. New policies can be created. Existing policies can be modified, deleted or copied.

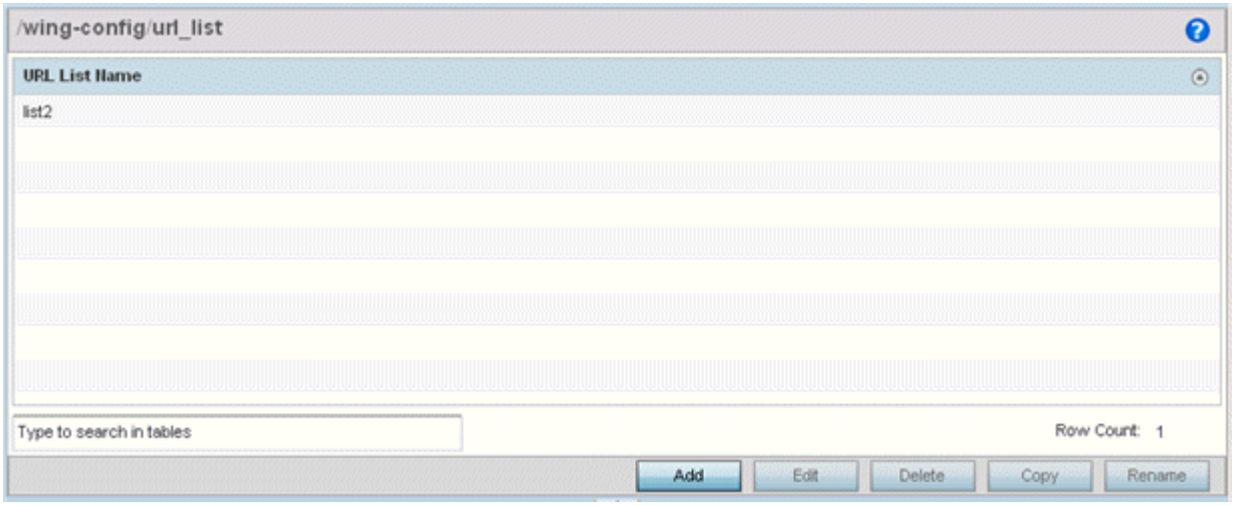



**Figure 410: Smart Caching - URL List Name Screen**

4 Refer to the **URL List Name** table to review the administrator assigned name applied to the URL list policy upon creation.

5 Select **Add** to create a URL lists policy. Select an existing policy and click **Edit** to modify, **Delete** to remove or **Copy** to copy the settings of a selected (existing) URL lists policy.

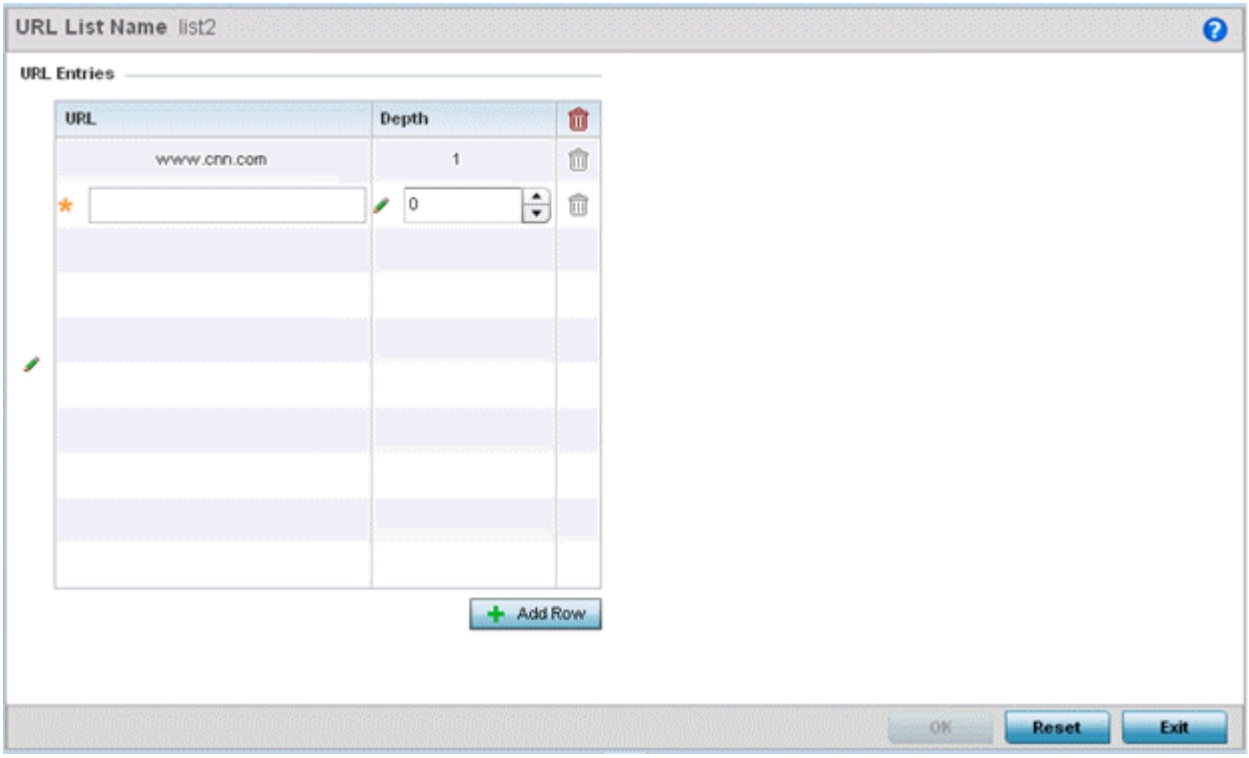



**Figure 411: URL List Name - Add/Edit Screen**

6 Select **+ Add Row** to display configurable parameters for defining a URL and its depth.

7 If you are creating a new URL lists policy, assign a name to it. The name cannot exceed 32 characters.

If you are editing an existing URL lists policy, the policy name cannot be modified.

8 Set the following **URL Lists** parameters:

| | |
|---|---|
| URL | Set the requested URL monitored and routed according to existing cache content policies. This value is mandatory. |
| Depth | Select the number of levels to be cached. Because Web sites have different parameters to uniquely identify specific content, the same content may be stored on multiple origin servers. Smart caching uses subsets of these parameters to recognize that the content is the same and serves it from cache. The available range is from 1 - 10. This value is mandatory. |

9 Select **OK** to save the URL Entries list configuration. Select **Reset** to revert to the last saved configuration.

## Setting the Imagotag Policy

SES-imagotag's ESL *(Electronic Shelf Label)* tags are small, battery-powered devices used by retail businesses to display information, such as product code, pricing, etc. These tags are activated, configured, and managed through an SES-Imagotag provided server. The tags and server communicate through an ESL communicator (a USB dongle), connected to the USB port on the WiNG AP. This communication is over the 2.4 GHz band using a proprietary RF protocol. The ESL communicator acts as a bridge between the tags and the server, using WiNG AP as an infrastructure device.

Use this option to enable support for SES-imagotag's ESL tags on WiNG APs with USB interfaces. In case of standalone AP's, apply the policy to the AP's self. In case of adopted APs, the policy is pushed to the AP through the adopting controller. In the latter case, apply the policy on the AP's profile.

An Imagotag-enabled AP recognizes the ESL communicator, and facilitates communication between communicator and tags.

Note
This feature is supported only on the AP-8432 model access point.

To navigate to the Imagotag Policy screen:

1 Select the **Configuration** tab from the main menu.

2 Select the **Services** tab from the Configuration menu.

The upper left-hand side of the user interface displays a Services menu pane where **`Captive Portal`**, **`DNS Whitelist`**, **`DHCP Server Policy`**, **`RADIUS`** , **`Guest Management`**, etc. configuration options can be selected.

3 Select the **Imagotag Policy** option.

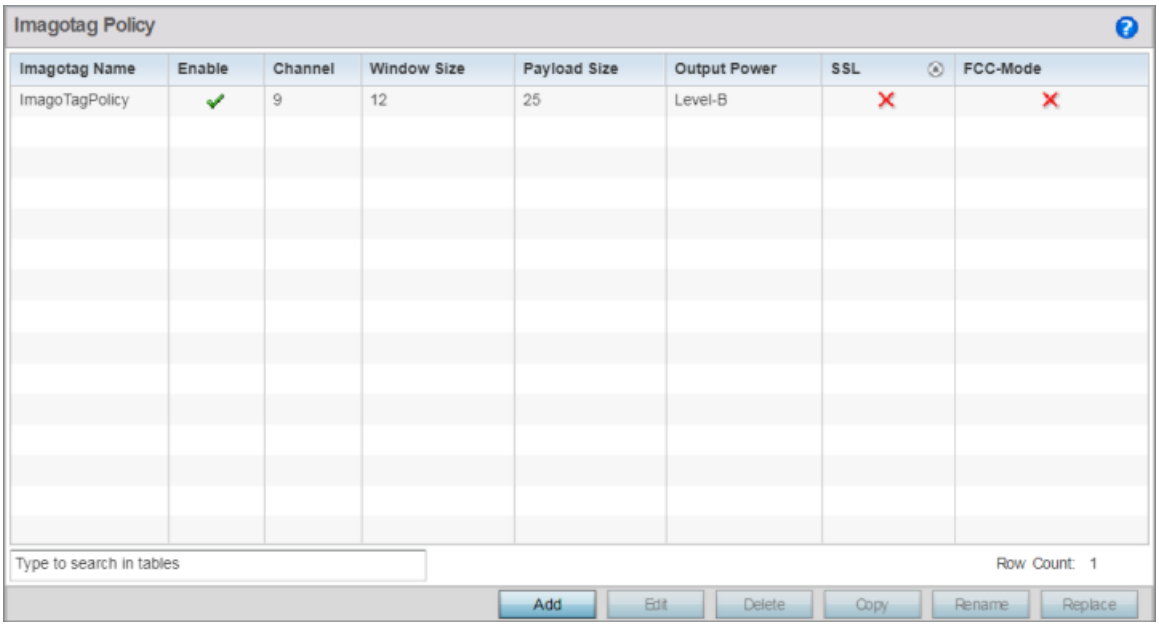



**Figure 412: Configuration - Services - Imagotag Policy screen**

4 Review the following existing Imagotag Policy settings, to determine whether a new policy requires creation, an existing policy requires modification or an existing policy requires deletion:

| | |
|---|---|
| Imagotag Name | Displays the Imagotag policy name. |
| Enable | Displays the status of the policy: Enabled/Disabled. A green check mark indicates that the policy is enabled. A red cross mark indicates that the policy is disabled. |
| Channel | Displays the channel assigned for ESL communicator to tag communication in the 2.4 GHz band. |
| Window Size | Displays the transmission window size for messages exchanged between ESL communicator and tags. |
| Payload Size | Displays the maximum payload size in packets exchanged between ESL communicator and tags. |
| Output Power | Displays the maximum output power set for the ESL communicator. |
| SSL | Displays if SSL *(Secure Socket Layer)* encryption mode of communication is enabled or not. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled. |
| FCC-Mode | Displays if the FCC compatibility mode is enabled or not on the ESL communicator. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled. |

## Adding/Editing Imagotag Policy Settings

To add/edit an Imagotag policy:

1 Select **Add** and create a new policy. To modify, remove, copy or rename and existing policy, select the policy from those listed on the screen and click the **Edit**, **Delete**, **Copy** or **Rename** button.

The Imagotag Policy add/edit screen displays.

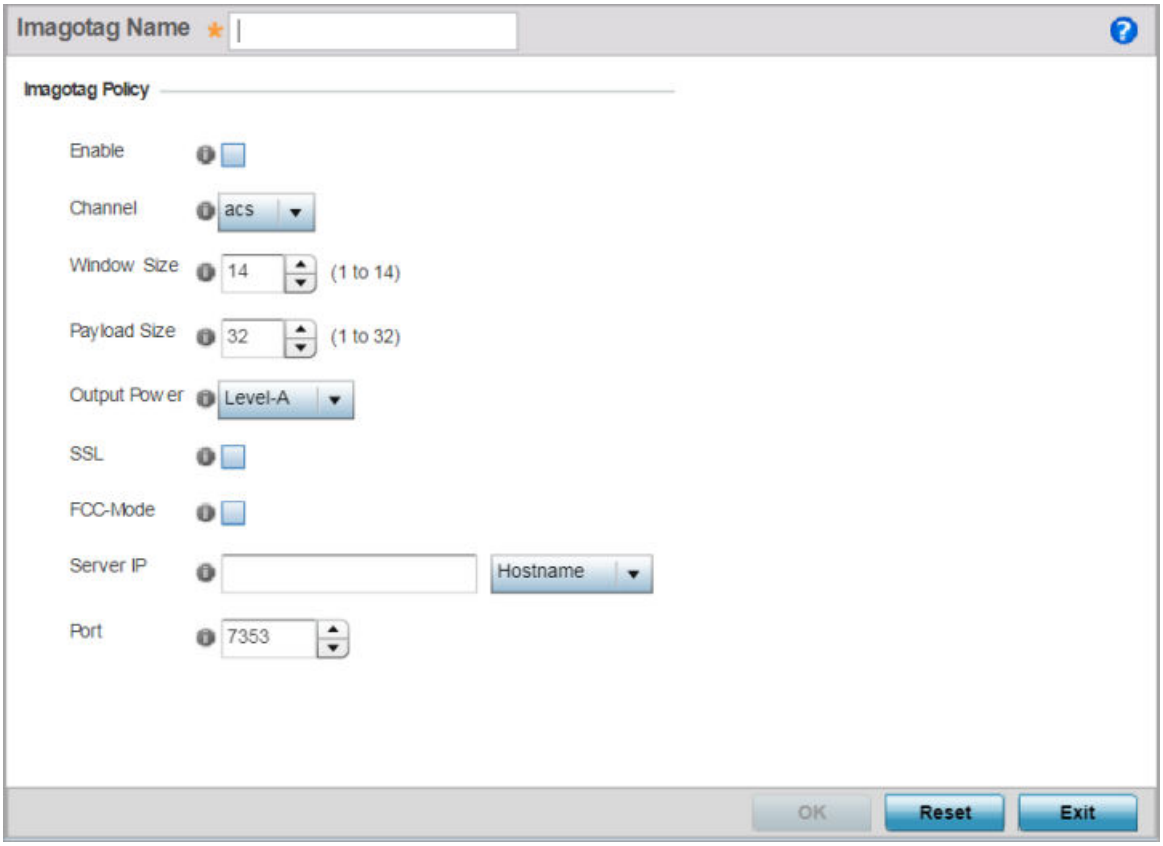



**Figure 413: Add/Edit Imagotag Policy screen**

2 If adding a new policy, in the Imagotag Name field, enter the policy name.

3 Configure or edit the following Imagotag policy settings:

| | |
|---|---|
| Enable | Select to enable the policy. |
| Channel | Use this drop-down menu to configure the channel assigned for the ESL communicator to tag communication in the 2.4 GHz band. The option are:<br>• ACS *(Auto-Channel Selection)* - Enables auto channel selection mode. This is the default setting.<br>• 0 - 10 - Sets the RF channel of operation within the 0-10 range. |
| Window Size | Use the spinner control to set the transmission window size for messages exchanged between ESL communicator and tags.<br>• 1-14 - Set a value between 1-14 bytes. The default value is 14 bytes.<br><br>Note: SES-Imagotags recommends NOT to change the default setting. |

| | |
|---|---|
| Payload Size | Use the spinner control to set the maximum size of the payload in packets exchanged between ESL communicator and tags.<br>• 1-32 - Specify the value from 1 - 32 bytes. The default setting is 32 bytes.<br><br>Note: SES-Imagotags recommends NOT to change the default setting. |
| Output Power | Use the spinner control to configure the maximum output power for the ESL communicator. The options are:<br>• Level-A – 1 dBm. This is the default setting.<br>• Level-B - -4 dBm<br>• Level-C - -6 dBm<br>• Level-D - -12 dBm<br>• Level-E - 0 dBm<br>• Level-F - -2 dBm<br>• Level-G - -8 dBm<br>• Level-H - -10 dBm<br><br>Note: SES-Imagotags recommends NOT to change the default setting, which is in conformance to various country/region specific RF regulations. |
| SSL | Select to enable secure, encrypted communication over the SSL *(Secure Socket Layer)* between the AP and SES-imagotag server. This option is disabled by default. |
| FCC-Mode | Select to enable the FCC *(Federal Communications Commission)* compatibility mode on the ESL communicator. This option is disabled by default. |
| Server ID | Use this field to specify the Imagotag server's IP address or hostname.<br>As per the current implementation, at the ESL server end, the WiNG AP's IP address was configured to enable the server contact the AP and establish connection with the ESL communicator (USB Dongle). Starting with WiNG 5.9.3, it is the AP that initiates communication with the ESL Imagotag server. The AP sends a connection request to the ESL server specified here. |
| Port | Use the spinner control to set the port on which the Imagotag server is reachable. The default value is 7353. |

4 Select **OK** to save the configurations. Select **Reset** to revert to the last saved configuration.

## Services Deployment Considerations

Before defining the access point's configuration using the Services menu, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- We recommend that each RADIUS client use a different shared secret password. If a shared secret is compromised, only the one client poses a risk as opposed all the additional clients that potentially share that secret password.
- Consider using an LDAP server as a database of user credentials that can be used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location.
- Designating at least one secondary server is a good practice to ensure RADIUS user information is available if a primary server were to become unavailable.

# 11 Management Access



Controllers, service platforms and access points have mechanisms to *allow* or *deny* device access for separate interfaces and protocols (*HTTP,HTTPS*, *Telnet*, *SSH* or *SNMP*). Management access can be *enabled* or *disabled* as required for unique policies. The Management Access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IP addresses to access specific interfaces.

Controllers and service platforms can be managed using multiple interfaces (SNMP, CLI and Web UI). By default, management access is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security, administrators can apply various restrictions as needed to:

- Restrict SNMP, CLI and Web UI access to specific hosts or subnets
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices
- Provide authentication for management users
- Apply access restrictions and permissions to management users

Management restrictions can be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of the device when guest services are deployed.

Note
Access points utilize a single Management Access policy, so ensure all the intended administrative roles, permissions, authentication and SNMP settings are correctly set. If an access point is functioning as a Virtual Controller AP, these are the access settings used by adopted access points of the same model as the Virtual Controller AP.

## Adding or Editing a Management Access Policy

To add a new Management Access policy, or edit an existing configuration:

1 Select **Configuration** → **Management** →**Management Policy** to display the main Management Policy screen and the Management Browser.
   - To modify an existing policy, select **Management Browser** > **Edit**.
   - To add a new policy, click **Add** on the bottom right-hand side of the Management screen.

2 Name the new policy to enable the Access Control, SNMP, SNMP Traps and Administrators tabs and define the policy configuration.
   The name cannot exceed 32 characters.

3 Click **OK** to commit the new policy name.

Once the new name is defined, the screen's tabs become enabled, with the contents of the Administrators tab displayed by default. Refer to the following to define the configuration of the new Management Access policy:

| | |
|---|---|
| Creating an Administrator Configuration | Use the Administrators tab to create specific users, assign them permissions to specific protocols and set specific administrative roles for the network. |
| Setting the Access Control Configuration | Use the Access Control tab to enable/disable specific protocols and interfaces. Again, this kind of access control is not meant to function as an ACL, but rather as a means to enable/disable specific protocols (HTTP, HTTPS, Telnet etc.) for each Management Access policy. |
| Setting the Authentication Configuration | Refer to the Authentication tab to set the authentication scheme used to validate user credentials with this policy. |
| Setting the SNMP Configuration | Refer to the SNMP tab to enable SNMPv2, SNMPv3 or both and define specific community strings for this policy. |
| Setting SNMP Trap Configuration | Use the SNMP Traps tab to enable trap generation for the policy and define trap receiver configurations. |

For deployment considerations and recommendations impacting a controller or service platform's Management Access policy configuration, refer to Management Access Deployment Considerations on page 863.

## Creating an Administrator Configuration

Management services (Telnet, SSHv2, HTTP, HTTPS and FTP) require administrators enter a valid username and password which is authenticated locally or centrally on a RADIUS server. SNMPv3 also requires a valid username and password which is authenticated by the SNMPv3 module. For CLI and Web UI users, the controller or service platform also requires user role information to know what permissions to assign.

- If local authentication is used, associated role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied RADIUS using vendor specific return attributes. If no role information is supplied by RADIUS, the controller or service platform applies default read-only permissions.

Administrators can limit users to specific management interfaces. During authentication, the controller or service platform looks at the user's access assignment to determine if the user has permissions to access an interface:

- If local authentication is used, role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied by RADIUS using vendor specific return attributes.

The controller or service platform also supports multiple RADIUS server definitions as well as fallback to provide authentication in the event of failure. If the primary RADIUS server is unavailable, the controller or service platform authenticates with the next RADIUS sever, as defined in the AAA policy. If a RADIUS server is not reachable, the controller or service platform can fall back to the local database for authentication. If both RADIUS and local authentication services are unavailable, read-only access can be optionally provided.

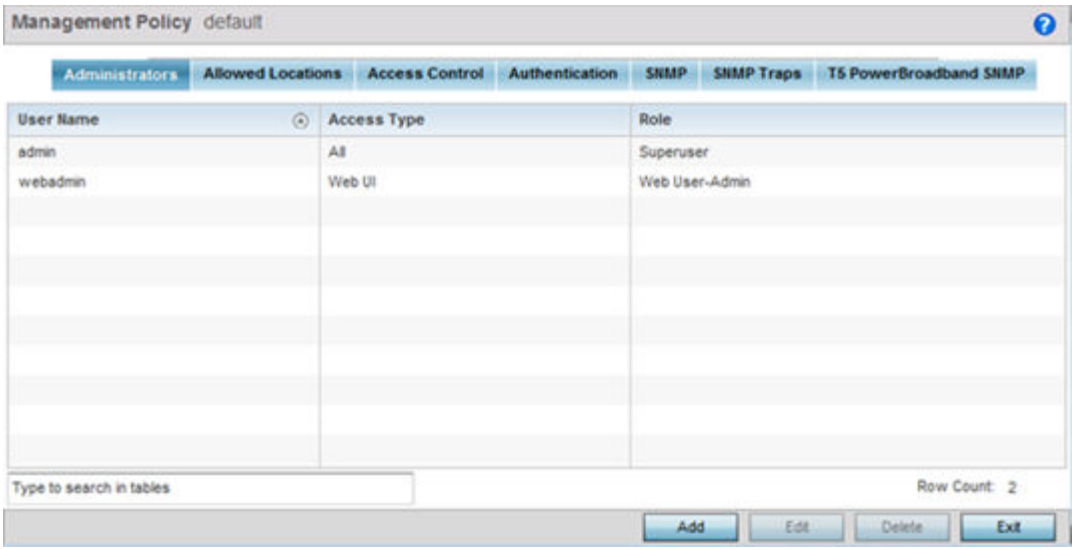
The controller or service platform authenticates users using the integrated local database. When user credentials are presented the controller or service platform validates the username and password against the local database and assigns permissions based on the associated roles assigned. The controller or service platform can also deny the authentication request if the user is attempting to access a management interface not specified in the account's access mode list.

Use the Administrators tab to review existing administrators, their access medium (type) and administrative role within the controller, service platform or access point managed network. New administrators can be added, and existing administrative user configurations modified or deleted as required.

To create administrators and assign them access types and roles:

1 Select the **Administrators** tab if not selected by default.

The Administrators screen displays.

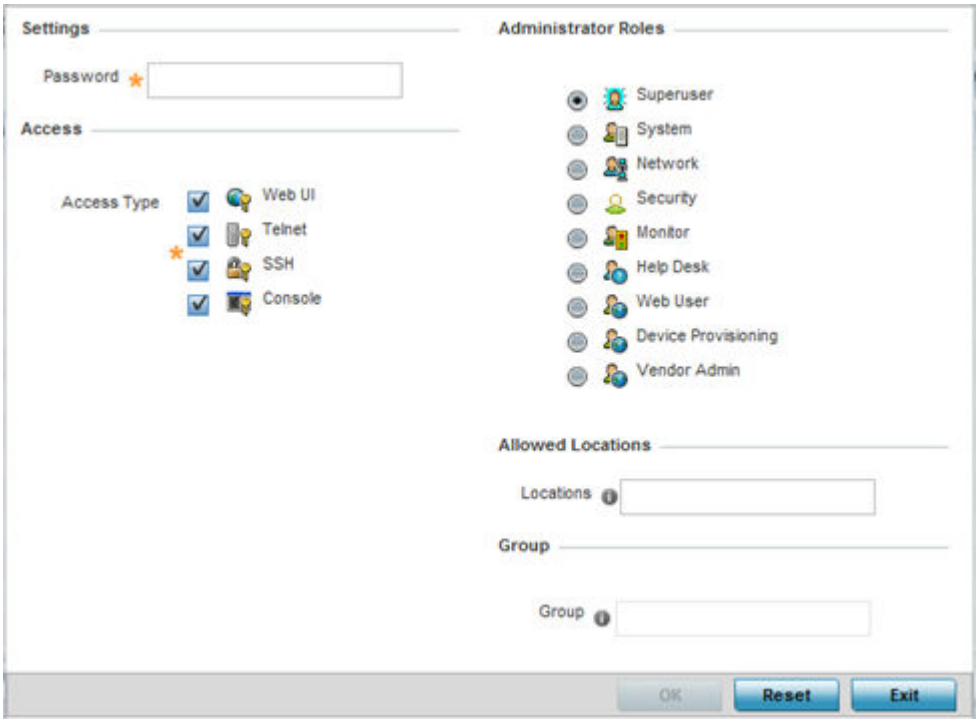



2 Refer to the following high-level configurations of existing administrators:

| | |
|---|---|
| User Name | Displays the name assigned to the administrator upon creation of their account. The name cannot be modified as part of the administrator configuration edit process. |
| Access Type | Lists the Web UI, Telnet, SSH or Console access type assigned to each listed administrator. A single administrator can have any one (or all) of these roles assigned at the same time. |
| Role | Lists the Superuser, System, Network, Security, Monitor, Help Desk, Web User, Device Provisioning or Vendor Admin role assigned to each listed administrator. An administrator can only be assigned one role at a time. |

3 Select **Add** to create a new administrator configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove an administrator from the list of those available.

The Administrators screen displays.




4 If creating a new administrator, enter a name in the User Name field.

This is a mandatory field for new administrators and cannot exceed 32 characters. Optimally assign a name representative of the user and role.

5 Provide a strong password for the administrator within the Password field. Reconfirm the password to ensure its accurately entered. This is a mandatory field.

6 Select **Access** options to define the permitted access for the user. Access modes can be assigned to management user accounts to restrict which management interfaces the user can access. A management user can be assigned one or more access roles allowing access to multiple management interfaces. If required, all four options can be selected and invoked simultaneously.

| | |
|---|---|
| Web UI | Select this option to enable access to the device's Web User Interface. |
| Telnet | Select this option to enable access to the device using TELNET. |
| SSH | Select this option to enable access to the device using SSH. |
| Console | Select this option to enable access to the device's console. |

7 Select the **Administrator Role** for the administrator using this profile. Only one role can be assigned.

| | |
|---|---|
| Superuser | Select this option to assign complete administrative rights to the user. This entails all the roles listed for all the other administrative roles. |
| System | The System role provides permissions to configure general settings like NTP, boot parameters, licenses, perform image upgrades, auto install, manager redundancy/clustering and control access. |

| | |
|---|---|
| Network | The Network role provides privileges to configure all wired and wireless parameters like IP configuration, VLANs, L2/L3 security, WLANs, radios, and captive portal. |
| Security | Select Security to set the administrative rights for a security administrator allowing configuration of all security parameters. |
| Monitor | Select Monitor to assign permissions without any administrative rights. The Monitor option provides read-only permissions. |
| Help Desk | Assign this role to someone who typically troubleshoots and debugs problems reported by the customer. The Help Desk manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views and retrieves logs. Help Desk personnel are ***not*** allowed to conduct controller or service platform reloads. |
| Web User | Select Web User to assign the administrator privileges needed to add users for authentication. |
| Device Provisioning | Select Device Provisioning to assign an administrator privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a device's existing configuration unless the configuration is properly archived.<br><br>Note:<br>Starting with WiNG 5.9.4, you can restrict a device provisioning admin's access to specific location or locations by applying the Allowed Locations tag. When applied, this user, will only have access to devices within the locations (RF Domains/sites/tree-node paths) associated with the allowed-locations tag.<br><br>Note: For information on configuring the allowed-locations tag, click here. |
| Vendor Admin | Select this option to create a vendor-admin user role group so this particular user type can access offline device-registration portal data. Vendors are assigned username/password credentials for securely on boarding devices. Devices are moved to a vendor allowed VLAN immediately after this on-boarding process, so vendors do require unique administration roles. When the Vendor-Admin role is selected, provide the vendor's Group name for RADIUS authentication. The vendor's RADIUS group takes precedence over the statically configured group for device registration.<br><br>Note: The Allowed Locations option is not applicable to this role. |

8 Use the Allowed Locations field to specify the allowed-locations tag. Each allowed-locations tag is mapped to one or multiple locations (RF Domains/sites/tree-node paths). By specifying an allowed-locations tag you are restricting the user's access to the location(s) mapped to the tag. However, in WiNG, this option is only applicable to the Device Provisioning user role.

9 Use the Group field to specify the user group to which this user belongs.

10 Click **OK** to save the administrator's configuration, or click **Reset** to revert to the last saved configuration.

## Setting the Access Control Configuration

Refer to the Access Control screen to allow/deny management access to the network using strategically selected protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Access options can be either enabled or

disabled as required. Consider disabling unused interfaces to close unnecessary security holes. The Access Control tab is not meant to function as an ACL (in routers or other firewalls), where you can specify and customize specific IPs to access specific interfaces.

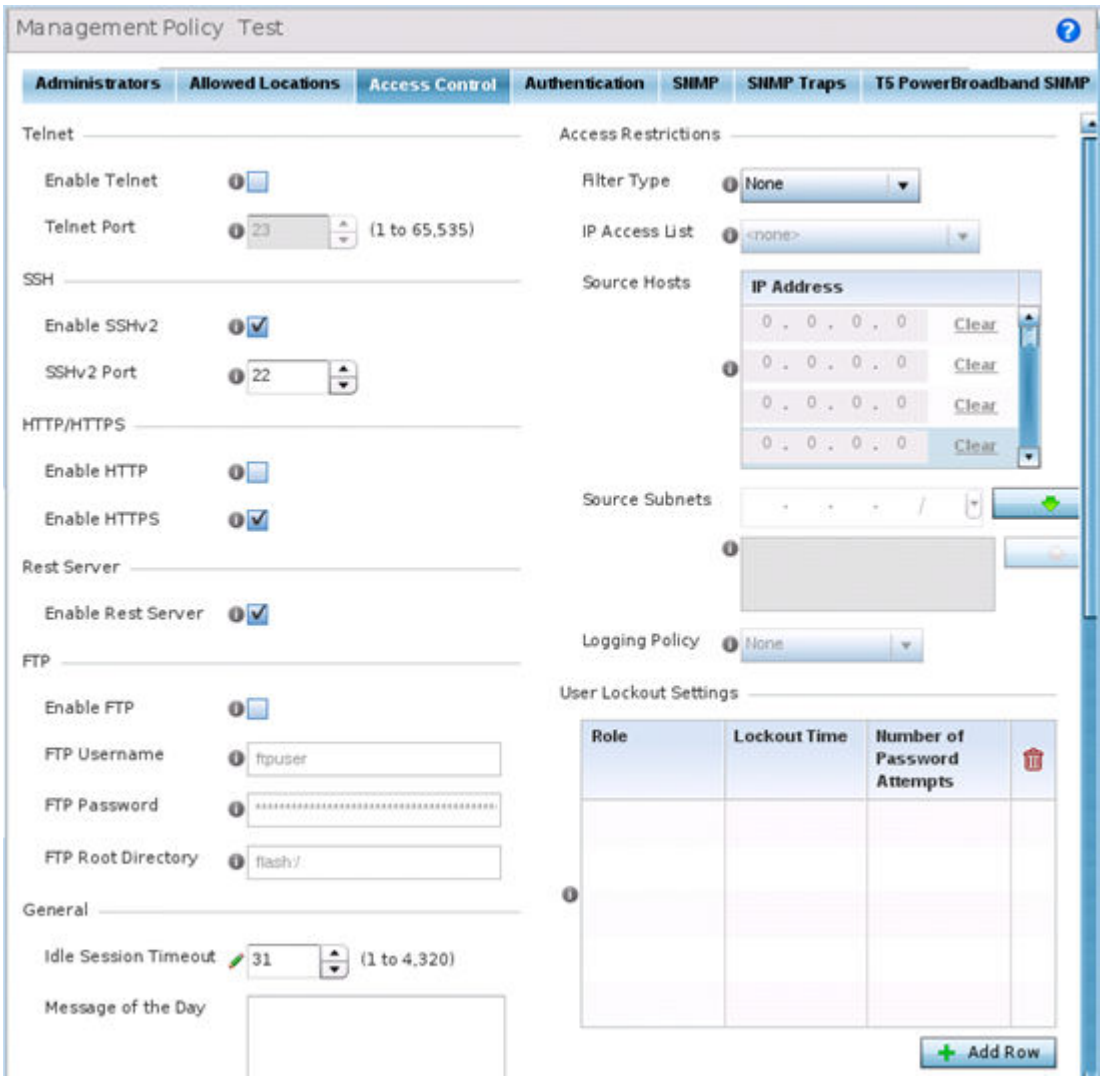
Administrators can secure access to a controller or service platform by disabling less secure interfaces. By default, the CLI, SNMP and FTP disable interfaces that do not support encryption or authentication. However, Web management using HTTP is enabled. Insecure management interfaces such as Telnet, HTTP and SNMP should be disabled, and only secure management interfaces, like SSH and HTTPS should be used to access the controller or service platform managed network.

The following table demonstrates how some interfaces provide better security than others:

| Access Type | Encrypted | Authenticated | Default State |
|---|---|---|---|
| Telnet | No | Yes | Disabled |
| SNMPv2 | No | No | Enabled |
| SNMPv3 | Yes | Yes | Enabled |
| HTTP | No | Yes | Disabled |
| HTTPS | Yes | Yes | Disabled |
| FTP | No | Yes | Disabled |
| SSHv2 | Yes | Yes | Disabled |

To set an access control configuration for the Management Access policy:

1 Select the Access Control tab.




2 Set the following parameters required for Telnet access:

| | |
|---|---|
| Enable Telnet | Select the checkbox to enable Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default. |
| Telnet Port | Set the port on which Telnet connections are made (1 - 65,535). The default port is 23. Change this value using the spinner control next to this field or by entering the port number in the field. |

3 Set the following parameters required for SSH access:

| | |
|---|---|
| Enable SSHv2 | Select the checkbox to enable SSH device access. SSH (Secure Shell) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default. |
| SSHv2 Port | Set the port on which SSH connections are made. The default port is 22. Change this value using the spinner control next to this field or by entering the port number in the field. |

4 Set the following HTTP/HTTPS parameters:

| | |
|---|---|
| Enable HTTP | Select the check box to enable HTTP device access. HTTP provides limited authentication and no encryption. |
| Enable HTTPS | Select the check box to enable HTTPS device access. HTTPS (Hypertext Transfer Protocol Secure) is more secure than plain HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication. |

Note
If the a RADIUS server is not reachable, HTTPS or SSH management access to the controller or service platform may be denied.

5 Set the following parameters required for FTP access:

| | |
|---|---|
| Enable FTP | Select the check box to enable FTP device access. FTP (File Transfer Protocol) is the standard protocol for transferring files over a TCP/IP network. FTP requires administrators enter a valid username and password authenticated locally on the controller. FTP access is disabled by default. |
| FTP Username | Specify a username required when logging in to the FTP server. The username cannot exceed 32 characters. |
| FTP Password | Specify a password required when logging in to the FTP server. Reconfirm the password in the field provided to ensure it has been entered correctly. The password cannot exceed 63 characters. |
| FTP Root Directory | Provide the complete path to the root directory in the space provided. The default setting has the root directory set to flash:/ |

6 Set the following **General** parameters:

| | |
|---|---|
| Idle Session Timeout | Specify an inactivity timeout for management connects (in seconds) between 1 - 4,320. The default setting is 12.0 |
| Message of the Day | Enter message of the day text (no longer than 255 characters) displayed at login for clients connecting via Telnet or SSH. |

7 Set the following **Access Restrictions** parameters:

| | |
|---|---|
| Filter Type | Select a filter type for access restriction. Options include IP Access List, Source Address or None. To restrict management access to specific hosts, select Source Address as the filter type and provide the allowed addresses within the Source Hosts field. |
| IP Access List | If the selected filter type is IP Access List, select an access list from the drop-down menu or select the Create button to define a new one. IP based firewalls function like Access Control Lists (ACLs) to filter/mark packets based on the IP from which they arrive, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies, so if you do not have an idea of what kind of access to allow or deny, a firewall is of little value, and could provide a false sense of network security. |
| Source Hosts | If the selected filter type is Source Address, enter an IP Address or IP Addresses for the source hosts. To restrict management access to specific hosts, select Source Address as the filter type and provide the allowed addresses within the Source Hosts field. |
| Source Subnets | If the selected filter type is Source Address, enter a source subnet or subnets for the source hosts. To restrict management access to specific subnets, select Source Address as the filter type and provide the allowed addresses within the Source Subnets field. |
| Logging Policy | If the selected filter is Source Address, enter a logging policy for administrative access. Options includes None, Denied Requests or All. |

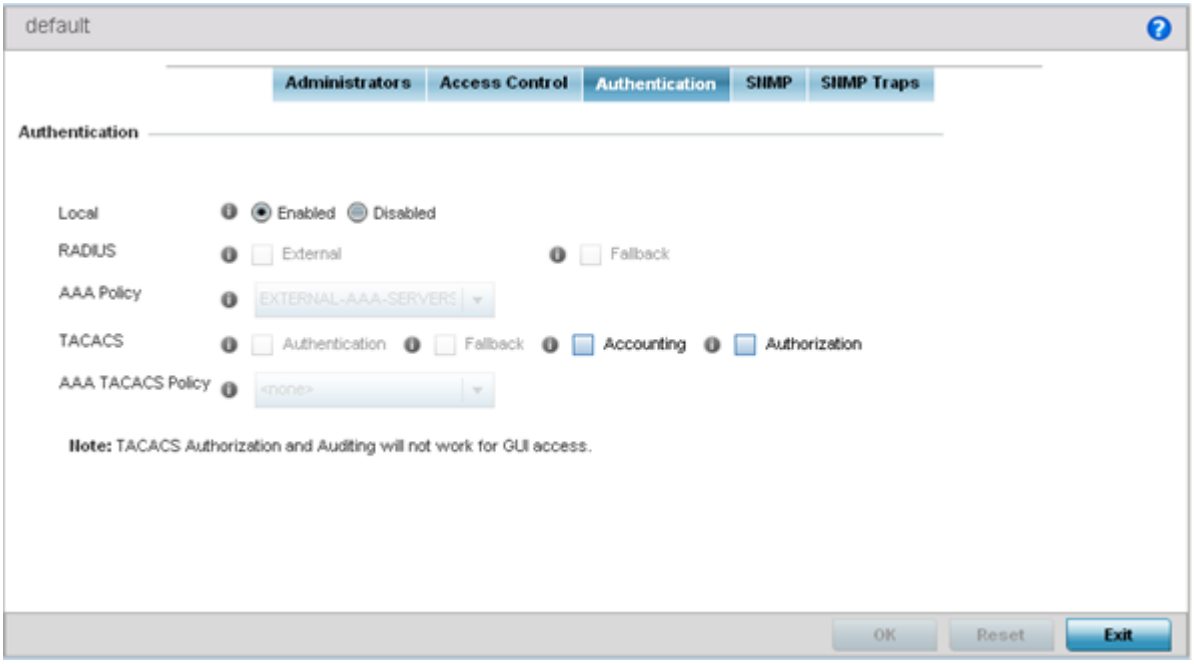
8 Click **OK** to save the Access Control configuration or click **Reset** to revert to the last saved configuration.

## Setting the Authentication Configuration

Refer to the Authentication tab to define how user credential validation is conducted on behalf of a Management Access policy. Setting up an authentication scheme by policy allows for policy member credential validation collectively, as opposed to authenticating users individually.

To configure an external authentication resource:

1 Select the Authentication tab.




2 Define the following settings to authenticate management access requests:

| | |
|---|---|
| Local | Select whether the authentication server resource is centralized (local), or whether an external authentication resource is used for validating user access requests. |
| RADIUS | If local authentication is disable, define whether the RADIUS server is *External* or *Fallback*. Select fallback to revert to local RADIUS resources should a dedicated external server be unreachable. |

3 Use the drop-down menu to specify to select the AAA Policy to use with an external RADIUS resource. Access points not using its local RADIUS resource will need to interoperate with a RADIUS and LDAP Server (AAA Servers) to provide user database information and user authentication data. If there is no AAA policy suiting your RADIUS authentication requirements, either select the **Create** icon to define a new AAA policy or select an existing policy from the drop-down menu and select the **Edit** icon to update its configuration.

4 Set the following AAA TACACS configuration parameters:

| | |
|---|---|
| Authentication | Select to enable TACACS authentication on login. This option is not available when the Local field is set to enabled. Also, this option cannot be selected when Fallback is selected. |
| Fallback | Select to enable fallback to use local authentication if TACACS authentication fails. This option is not available when the Local field is set to enabled. Also, this option cannot be selected when Authentication is selected. |
| Accounting | Select to enable TACACS accounting on login. This option is not available when the Local field is set to enabled. When selected, the AAA TACACS Policy field is enabled. |

| | |
|---|---|
| Authorization | Select to enable TACACS authorization on login. |
| Authorization Fallback | Select to enable fallback on TACACS authorization failure. This option is only available when Authorization is selected. |

5 Configure the AAA TACACS Policy to use with this authentication policy. Use the drop-down to select a configured AAA TACACS policy.

6 Click **OK** to update the authentication configuration, or click **Reset** to revert to the last saved configuration.

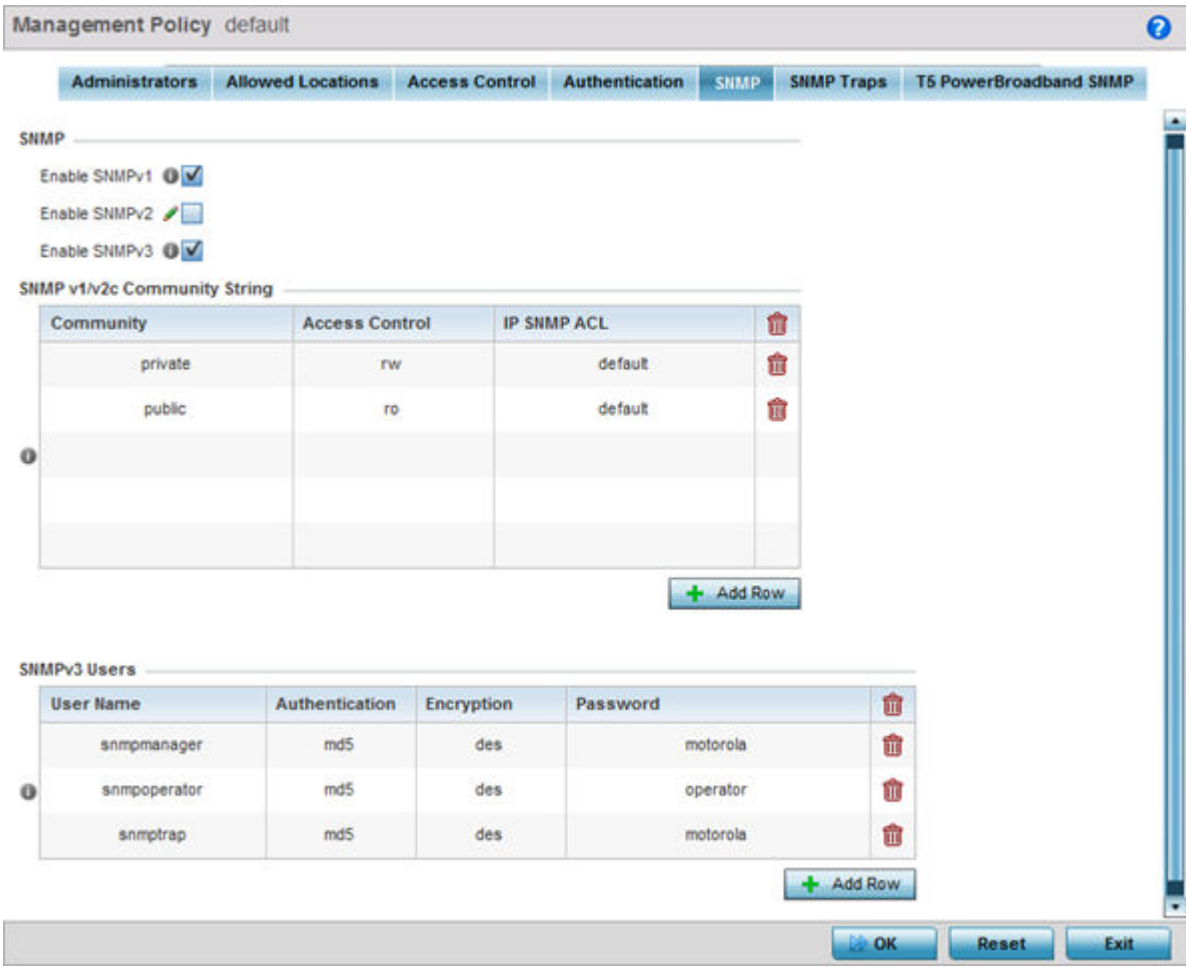
## Setting the SNMP Configuration

Optionally use the *Simple Network Management Protocol* (SNMP) to communicate with controllers, service platforms and access points within the wireless network. SNMP is an application layer protocol that facilitates the exchange of management information to and from a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to *set* device parameters. SNMP is generally used to monitor a system's performance and other parameters.

| SNMP Version | Encrypted | Authenticated | Default State |
|---|---|---|---|
| SNMPv1 | No | No | Disabled |
| SNMPv2 | No | No | Enabled |
| SNMPv3 | Yes | Yes | Enabled |

To configure SNMP Management Access:

1 Select the SNMP tab.




2 Enable or disable SNMP v1, SNMPv2 and SNMPv3.

| | |
|---|---|
| Enable SNMPv1 | SNMP v1exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified as text strings, with version 1 being the original (rudimentary) implementation. SNMPv1 is enabled by default. |
| Enable SNMPv2 | Select the checkbox to enable SNMPv2 support. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses Get, GetNext, and Set operations for data management. SNMPv2 is enabled by default. |
| Enable SNMPv3 | Select the checkbox to enable SNMPv3 support. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *user-based security model* (USM) for message security and the *view-based access control model* (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default. |

3 Set the SNMP v1/v2 Community String configuration. Use the + Add Row function as needed to add additional SNMP v1/2 community strings, or select an existing community string's radio button and select the **Delete** icon to remove it.

| | |
|---|---|
| Community | Define a **public** or **private** community designation. By default, SNMPv2 community strings on most devices are set to public, for the read-only community string, and private for the read-write community string. |
| Access Control | Set the access permission for each community string used by devices to retrieve or modify information. Available options include:<br>• Read Only - Allows a remote device to retrieve information.<br>• Read-Write - Allows a remote device to modify settings. |
| IP SNMP ACL | Set the IP SNMP ACL used along with community string. Use the dropdown menu to select an existing ACL. Use the Create icon to create and add a new ACL. Select an existing ACL and the Edit icon to update an existing ACL. |

4 Set the SNMPv3 Users configuration. Use the **+ Add Row** function as needed to add additional SNMPv3 user configurations, or select a SNMP user and select the Delete icon to remove the user.

| | |
|---|---|
| User Name | Use the drop-down menu to define a user name of snmpmanager, snmpoperator or snmptrap. |
| Authentication | Displays the authentication scheme used with the listed SNMPv3 user. The listed authentication scheme ensures only trusted and authorized users and devices can access the network. |
| Encryption | Select to enable TACACS accounting on login. This option is not available when the Local field is set to enabled. When selected, the AAA TACACS Policy field is enabled. |
| Password | Provide the user's password in the field provided. Select the Show check box to display the actual character string used in the password, while leaving the check box unselected protects the password and displays each character as "*". |

5 Select **OK** to update the SNMP configuration. Select Reset to revert to the last saved configuration.

## Setting SNMP Trap Configuration

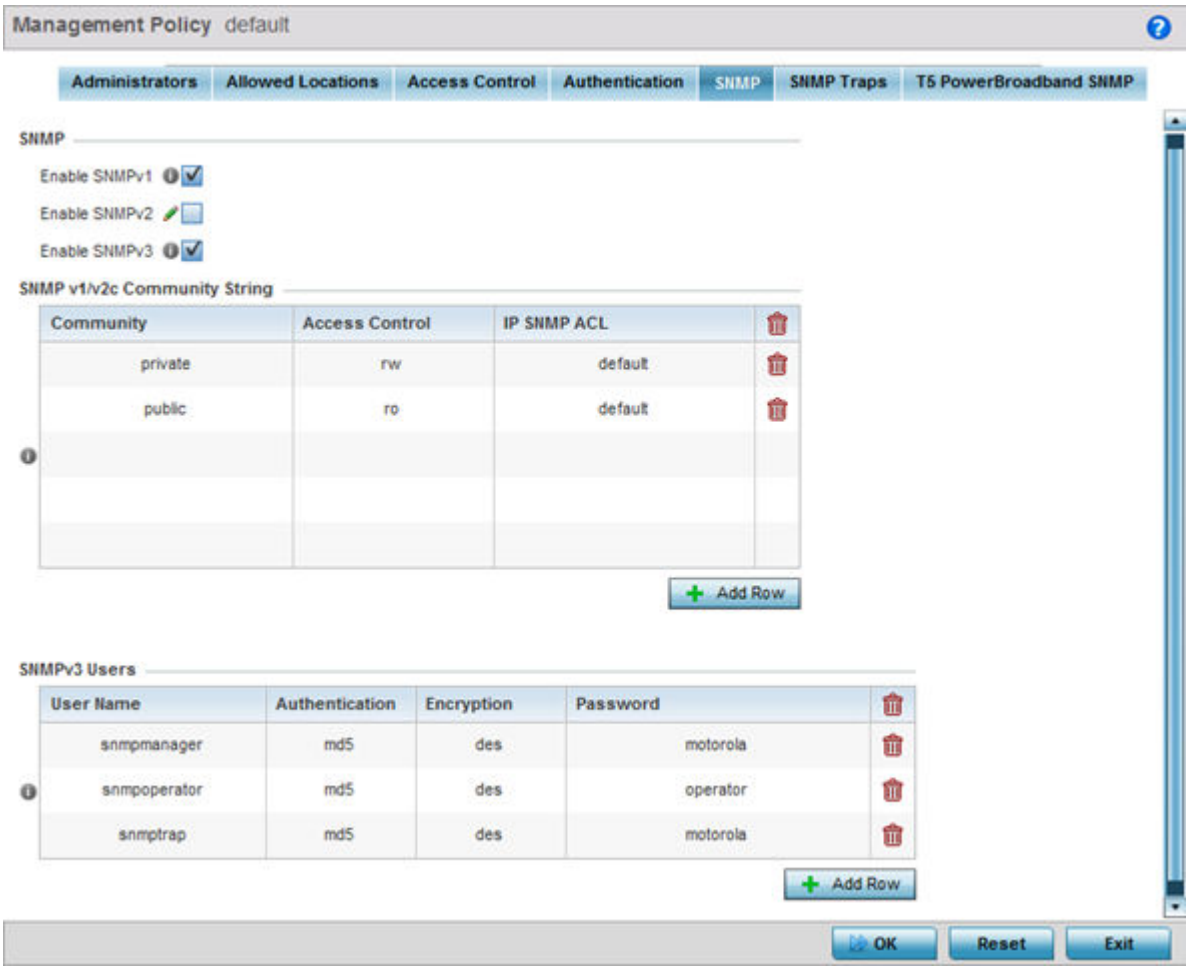
Controller, service platform and access point managed networks use SNMP trap receivers for fault notifications. SNMP traps are unsolicited notifications triggered by thresholds (or actions), and are an important fault management tool.

A SNMP trap receiver is the defined destination for SNMP messages (external to the controller,service platform or access point). A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community etc.

SNMP trap notifications exist for most operations, but not all are necessary for day-to-day operation.

To define a SNMP trap configuration for receiving events at a remote destination:

1 Select the SNMP Traps tab.




2 Select the **Enable Trap Generation** checkbox to enable trap generation using the trap receiver configuration defined. This feature is disabled by default.

3 Refer to the Trap Receiver table to set the configuration of the external resource dedicated to receive trap information. Select **Add Row +** as needed to add additional trap receivers. Select the **Delete** icon to permanently remove a trap receiver.

| | |
|---|---|
| IP Address | Sets the IP address of an external server resource dedicated to receive SNMP traps on behalf of the controller, service platform or access point. |
| Port | Set the virtual port of the server resource dedicated to receiving SNMP traps. The default port is port 162. |
| Version | Sets the SNMP version to use to send SNMP traps. SNMPv2 is the default. |
| Trap Community | Provide a 32 character maximum trap community string. The community string functions like a user id or password allowing access to controller or access point resources. If the community string is correct, the controller or access point provides with the requested information. If the community string is incorrect, the device controller or access point discards the request and does not respond. Community strings are used only by devices which support SNMPv1 and SNMPv2c. SNMPv3 uses username/password authentication, along with an encryption key. The default setting is **`public`**. |

4 Select **OK** to update the SNMP Trap configuration. Select **Reset** to revert to the last saved configuration.

## Management Access Deployment Considerations

Before defining an access control configuration as part of a Management Access policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Unused management protocols should be disabled to reduce a potential attack against managed resources. For example, if a device is only being managed by the Web UI and SNMP, there is no need to enable CLI interfaces.
- Use management interfaces providing encryption and authentication. Management services like HTTPS, SSH and SNMPv3 should be used when possible, as they provide both data privacy and authentication (as opposed to HTTP which does not).
- By default, SNMPv2 community strings on most devices are set to *public* for the read-only community string and *private* for the read-write community string. Legacy devices may use other community strings by default.
- SNMPv3 should be used for device management, as it provides both encryption and authentication (both unavailable together in HTTP).
- Enabling SNMP traps can provide alerts for isolated attacks at both small managed radio deployments or distributed attacks occurring across multiple managed sites.
- Whenever possible, centralized RADIUS management be enabled. This provides better management and control of user names and passwords, and allows administrators to quickly change credentials in the event of a security breach.

# 12 Diagnostics

**Fault Management**
**Crash Files**
**Advanced**

Resident diagnostic capabilities enable administrators to understand how devices are performing and troubleshoot issues impacting device performance. Performance and diagnostic information is collected and measured on controllers and service platforms for any anomalies potentially causing a key processes to fail.

An access point's resident diagnostic capabilities enable administrators to understand how devices are performing and troubleshoot issues impacting network performance. Performance and diagnostic information is collected and measured for anomalies causing a key processes to potentially fail.

Numerous tools are available within the Diagnostics menu. Some allow event filtering, some enable log views and some allow you to manage files generated when hardware or software issues are detected.

Diagnostic capabilities include:

- Fault Management
- Crash Files
- Advanced

## Fault Management

Fault management enables user's administering multiple sites to assess how individual devices are performing and review issues impacting the network. Use the Fault Management screens to administrate errors generated by a controller, service platform, access point or wireless client.

### Filter Events

To conduct fault management on an access point:

1 Select **Diagnostics** > **Fault Management** > **Filter Events**.

The screen displays by default. Use this screen to configure how events are tracked. By default, all events are enabled, and an administrator has to turn off events that do not require tracking.

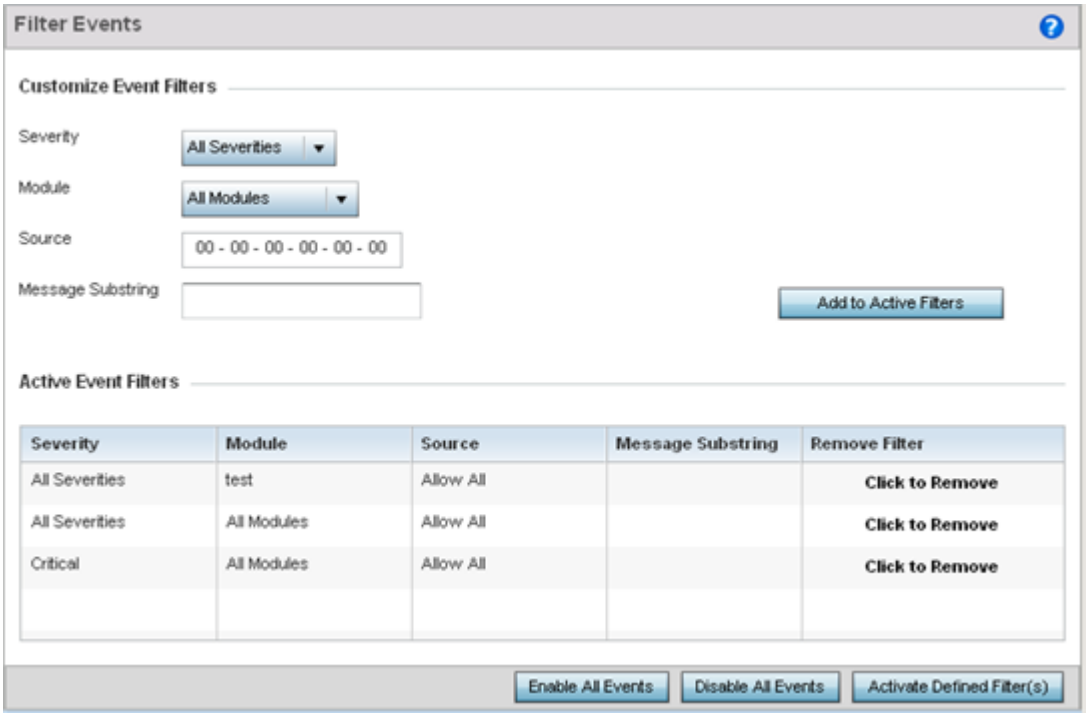



**Figure 414: Fault Management - Filter Events screen**

2 Use the Filter Events screen to create filters for managing detected events. Events can be filtered based on severity, module received, source MAC, device MAC and client MAC address.

3 Define the following **Customize Event Filters** parameters for the Fault Management configuration:

| | |
|---|---|
| Severity | Set the filtering severity. Select from the following:<br>*All Severities* – All events are displayed, irrespective of their severity<br>*Critical* – Only critical events are displayed<br>*Error* – Only errors and above are displayed<br>*Warning* – Only warnings and above are displayed<br>*Informational* – Only informational and above events are displayed |
| Module | Select the module from which events are tracked. When a module is selected, events from other modules are not tracked. Remember this when interested in events generated by a particular module. Individual modules can be selected (such as *TEST*, *LOG*, *FSM* etc.) or all modules can be tracked by selecting *All Modules*. |
| Source | Set the MAC address of the source device to be tracked. Setting a MAC address of 00:00:00:00:00:00 allows all devices to be tracked. |
| Message Substring | Optionally append a text message (substring) to the event filter to assist the administrator in distinguishing this filter from others with similar attributes. |

Note
Leave the fields to a default value of 00:00:00:00:00:00 to track all MAC addresses.

4 Select the **Add to Active Filters** button to create a new filter and add it to the **Active Event Filters** table. When added, the filter uses the current configuration defined in the Customize Event Filters field.

5 Refer to the **Active Event Filters** table table to set the following parameters:

a To activate all the events in the **Active Events Filters** table, select the **Enable All Events** button. To stop event generation, select **Disable All Events**.

b To enable an event in the **Active Event Filters** table, select the event, then select the **Activate Defined Filter(s)** button.

Note
Filters cannot be persisted across sessions. They must be created every time a new session is established.

## View Events

Individual events can be assessed for impact and administered based on their recency and severity. Review events and, if necessary, update the manner in which they're displayed.

To review diagnostic events:

1 Select **Diagnostics** > **Fault Management** > **View Events**.

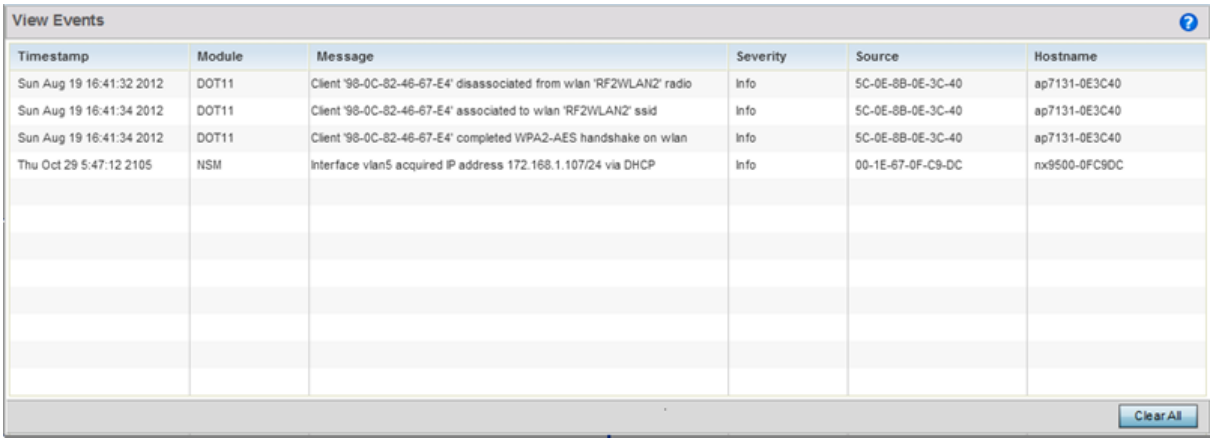



**Figure 415: Fault Management - View Events screen**

Use the View Events screen to track and troubleshoot events using the source and severity levels defined in the configure events screen.

2 Refer to the following event parameters to assess nature and severity of the displayed:

| | |
|---|---|
| Timestamp | Displays the Timestamp (time zone specific) when the fault occurred. |
| Module | Displays the module used to track the event. Events detected by other module are not tracked. |
| Message | Displays error or status messages for each event listed. |
| Severity | Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include:<br>*All Severities* – All events are displayed irrespective of their severity<br>*Critical* – Only critical events are displayed<br>*Error* – Only errors and above are displayed<br>*Warning* – Only warnings and above are displayed<br>*Informational* – Only informational and above events are displayed |

| | |
|---|---|
| Source | Displays the MAC address of the source device tracked by the selected module. |
| Hostname | Displays the Hostname/IP address of the source device tracked by the selected module. |

3 Select **Clear All**to clear the events displayed on this screen and begin a new event data collection.

## Event History

The Event History screen displays events for both wireless controllers and access points. The Controller(s) tab displays by default. Information on this tab can be filtered by controllers and then further by the RF Domains on the selected controller. Similarly, the access point(s) tab displays information for each RF Domain on the access point and this information can be further filtered on the devices adopted by this access point.

To review the Event History:

1 Select **Diagnostics** > **Fault Management** > **Event History**

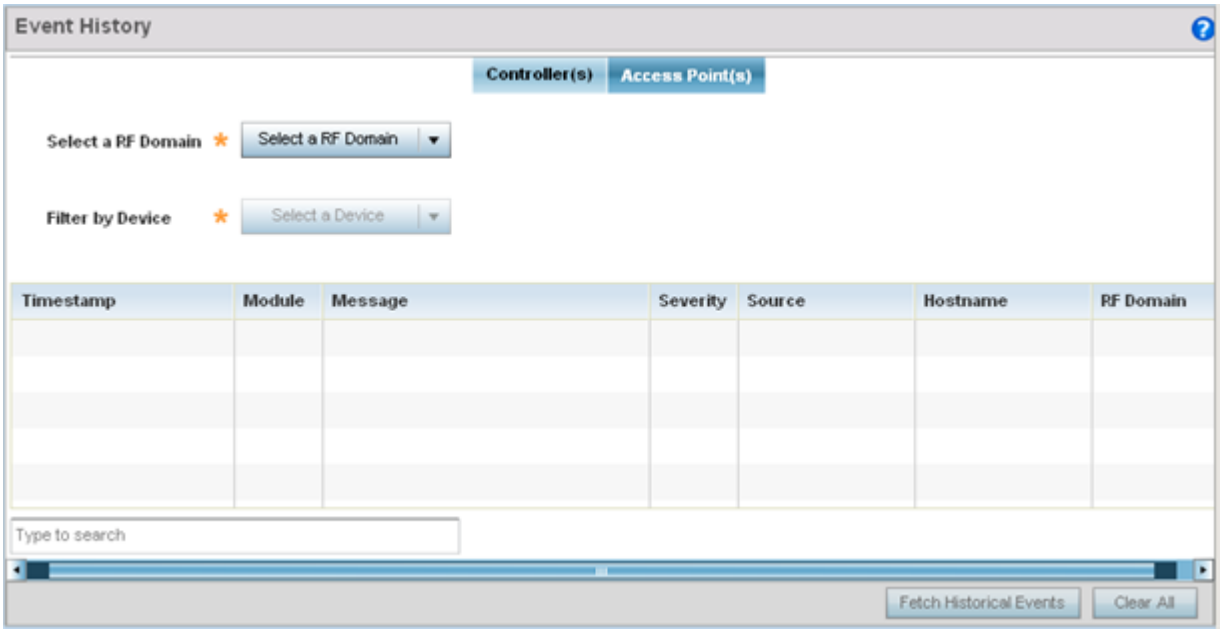



**Figure 416: Fault Management - Event History screen**

2 In the Controller(s) tab, select the controller from the **Select a Controller** field to filter events to display. To filter messages further, select a RF Domain from the **Filter by RF Domain** field.

3 In the access point(s) tab, select the RF Domain from the **Select a RF Domain** field to filter events to display. To filter messages further, select a device from the **Filter by Device** field.

4 Select **Fetch Historical Events** from the lower, right-hand, side of the UI to populate the table with either device or RF Domain events. The following event data is fetched and displayed:

| | |
|---|---|
| Timestamp | Displays the timestamp (time zone specific) each listed event occurred. |
| Module | Displays the module tracking the listed event. Events detected by other modules are not tracked. |
| Message | Displays error or status messages for each event. |

| | |
|---|---|
| Severity | Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include:<br>*All Severities* – All events are displayed irrespective of their severity<br>*Critical* – Only critical events are displayed<br>*Error* – Only errors and above are displayed<br>*Warning* – Only warnings and above are displayed<br>*Informational* – Only informational and above events are displayed |
| Source | Displays the MAC address of the device tracked by the selected module. |
| Hostname | Displays the Hostname/IP address of the device tracked by the selected module. |
| RF Domain | Displays the RF Domain where the selected access point MAC address resides. |

5 Select **Clear All** to clear events and begin new event data gathering.

## Crash Files

Use **Crash Files** to assess critical access point failures and malfunctions.

Use crash files to troubleshoot issues specific to the device on which a crash event was generated. These are issues impacting the core (distribution layer). Once reviewed, files can be deleted or transferred for archive. Crash files can be sent to a support team to expedite issues with the reporting device.

To review crash files impacting the access point network:

1 Select **Diagnostics** > **Crash Files**

The Crash Files screen displays a list of device MAC addresses impacted by core dumps.

2 Select a device from those displayed in the lower, left-hand, side of the UI.

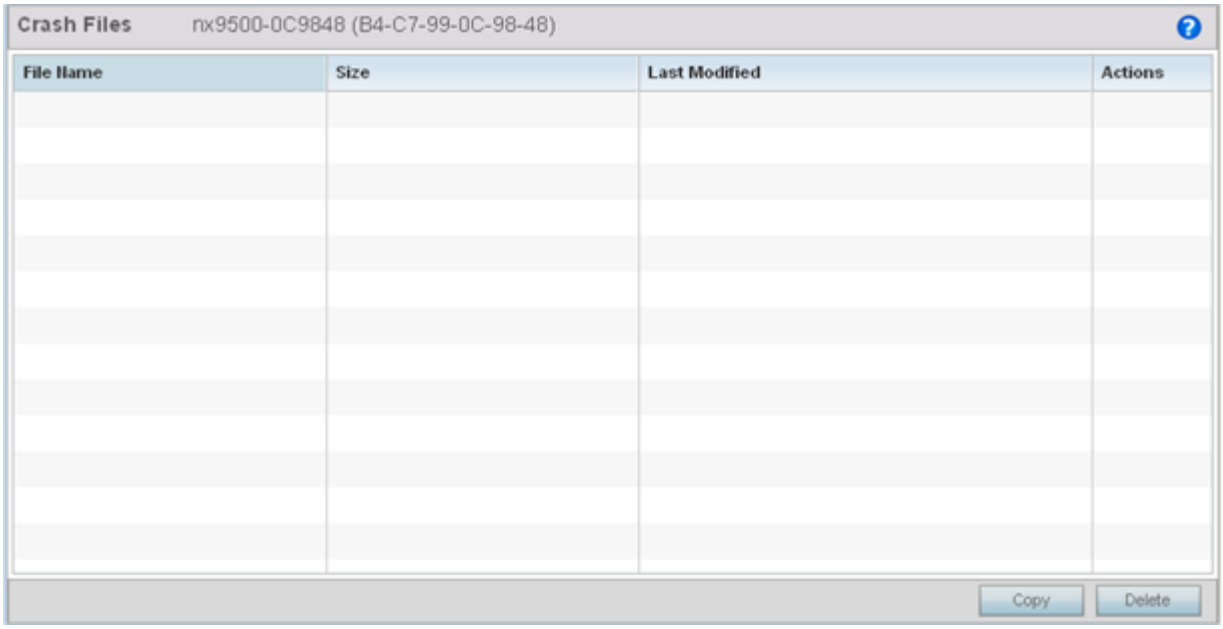



**Figure 417: Crash Files screen**

3 Refer to the following to review the following for each reported file:

| | |
|---|---|
| File Name | Displays the name of the file generated when a crash event occurred. This is the file available for copy to an external location for archive and remote administration. |
| Size | Lists the size of the crash file, as this information is often needed when copying files to an external location. |
| Last Modified | Displays the time stamp of the most recent update to the file. |
| Actions | Displays the action taken in direct response to the detected crash event. |

4 Select **Copy** to copy a selected crash file to an external location. Select **Delete** to remove a selected crash file.

# Advanced

Use Advanced diagnostics to review and troubleshoot potential issues with the access point's *User Interface* (UI). The UI Diagnostics screen contains tools to effectively identify and correct access point UI issues. Diagnostics can also be performed at the device level for connected clients.

The following options are available under the Advanced menu:

- UI Debugging on page 869
- Viewing UI Logs on page 870
- View Sessions on page 872

## UI Debugging

Use the **UI Debugging** screen to view debugging information for a selected device.

To review device debugging information:

1 Select **Diagnostics** > **Advanced** > **UI Debugging**

By default, **NETCONF Viewer** is selected.

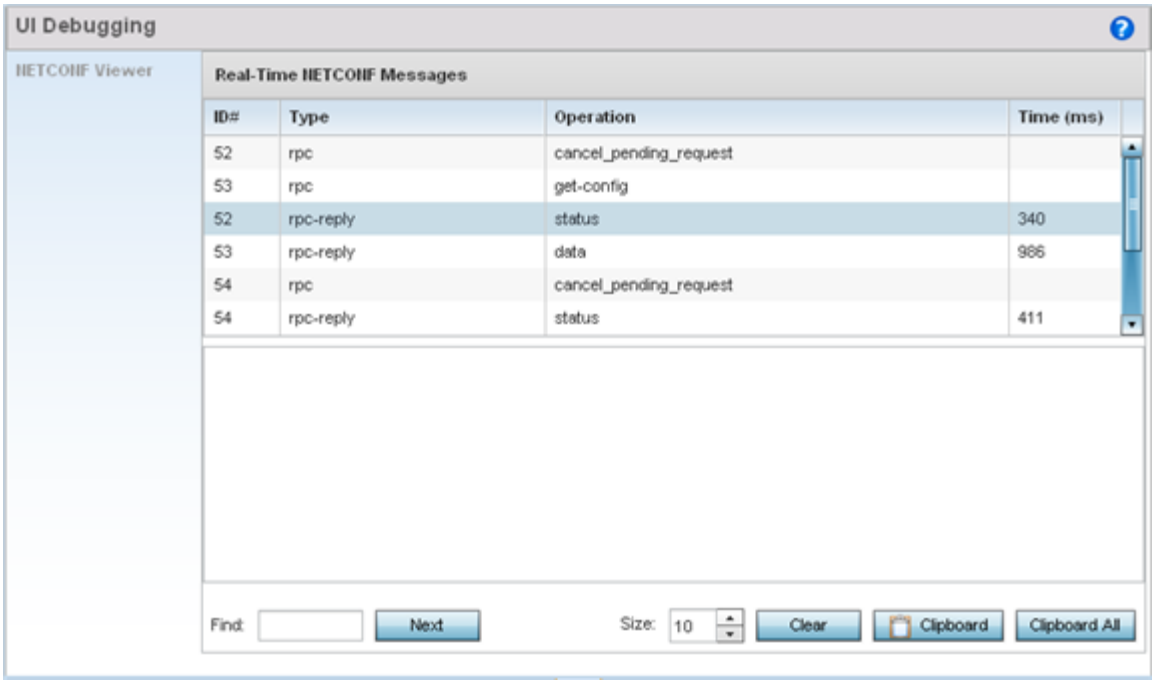



**Figure 418: UI Debugging screen - NETCONF Viewer**

2 Select a target ID to view its debugging information displays within the **NETCONF Viewer** screen.

3 Use **NETCONF Viewer** to review NETCONF information. NETCONF is a tag-based configuration protocol. Messages are exchanged using XML tags.

The **Real Time NETCONF Messages** area lists an XML representation of any message generated by the system. The main display area of the screen is updated in real time.

4 Use the **Clear** button to clear the contents of the **Real Time NETCONF Messages** area. Use the **Find** parameter and the **Next** button to search for message variables in the **Real Time NETCONF Messages** area.

Use the **Clipboard** button to copy the current selected message to the clipboard memory of the device used to access the user interface. Use the **Clipboard All** button to copy all the displayed messages to the clipboard memory.

## Viewing UI Logs

Use the **View UI Logs**screen to view the log messages generated by the device. Logs are classified as Flex Logs and Error Logs. These logs provide a real-time look into the state of the device and provide useful information for debugging and trouble shooting issues.

To display the logs:

1 Select **Diagnostics** > **Advanced** > **Viewing UI Logs**.

By default, the Flex Logs screen displays.

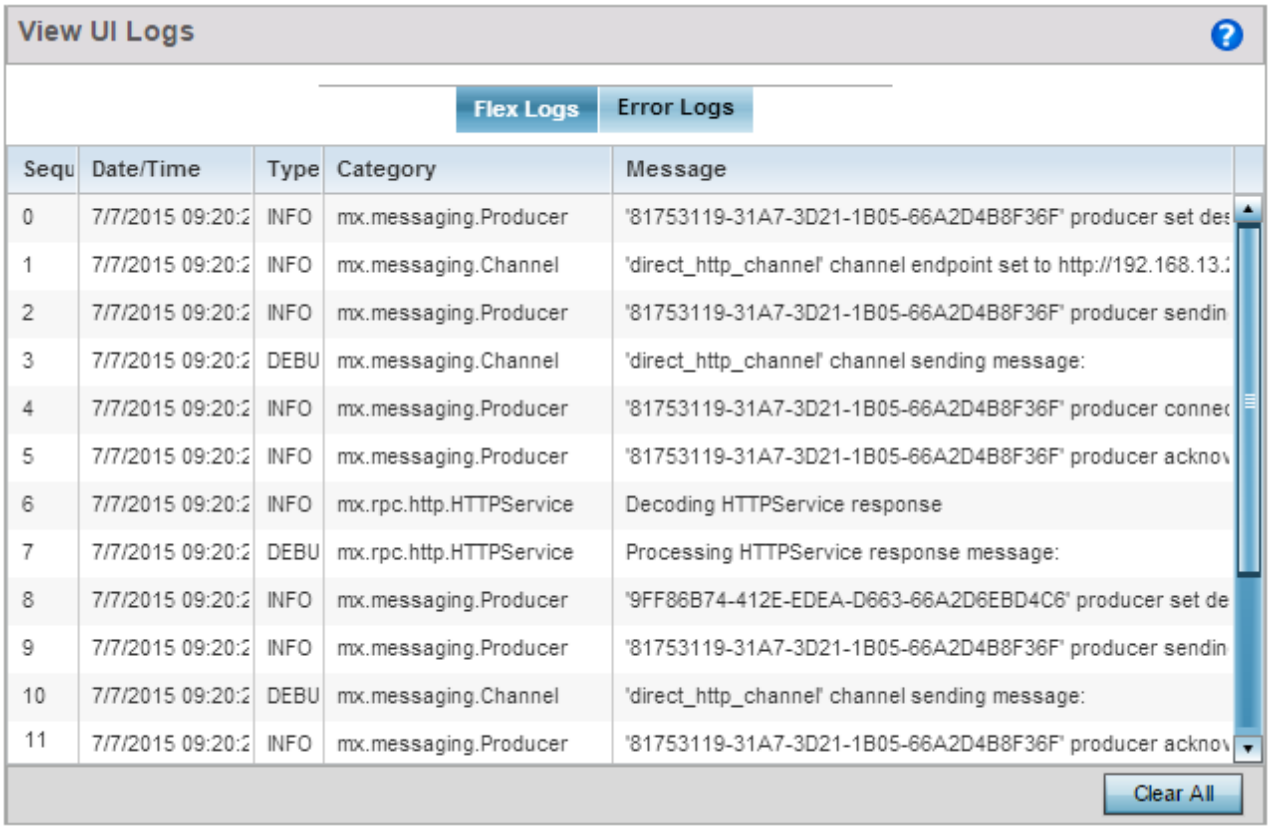



**Figure 419: View UI Logs - Flex Logs tab**

2 The sequence (order of occurrence), Date/Time, Type, Category and Message items display for each application log, flex log or error log selected.

Use the **Clear All** button to clear all logs shown in this screen.

3 Select the **Error Logs** tab to display the error logs for this device.

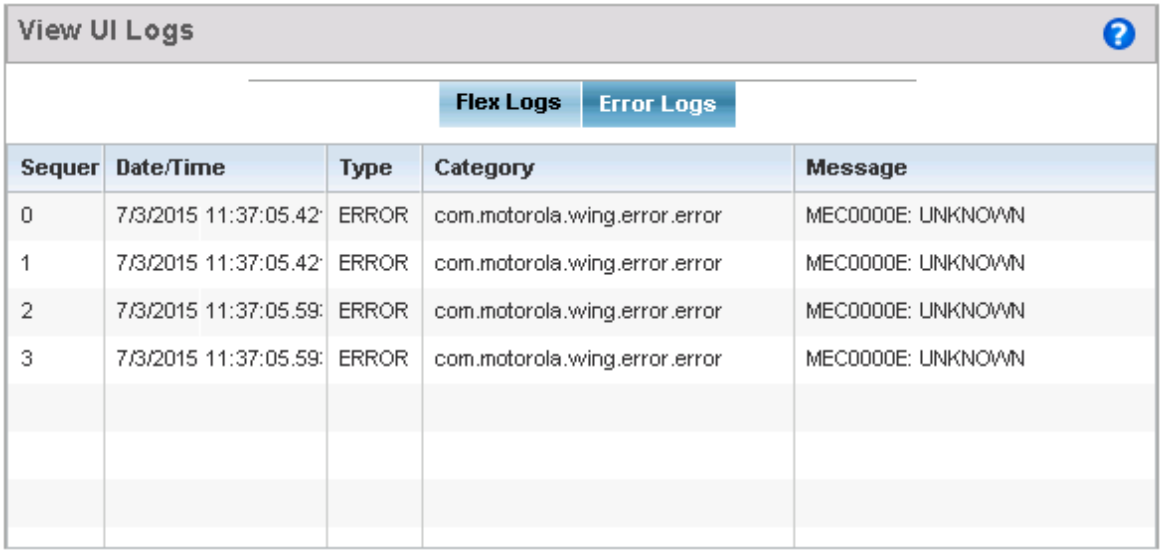



**Figure 420: View UI Logs - Error Logs tab**

The Sequence (order of occurrence), Date/Time, Type, Category and Message items display for each log option selected.

## View Sessions

The **View Sessions** displays a list of all sessions associated with this device. A session is created when a user name/password combination is used to access the device to interact with it for any purpose. Use the following to view a list of sessions associated with this device:

1 Select **Diagnostics** > **Advanced** > **View Sessions**

2

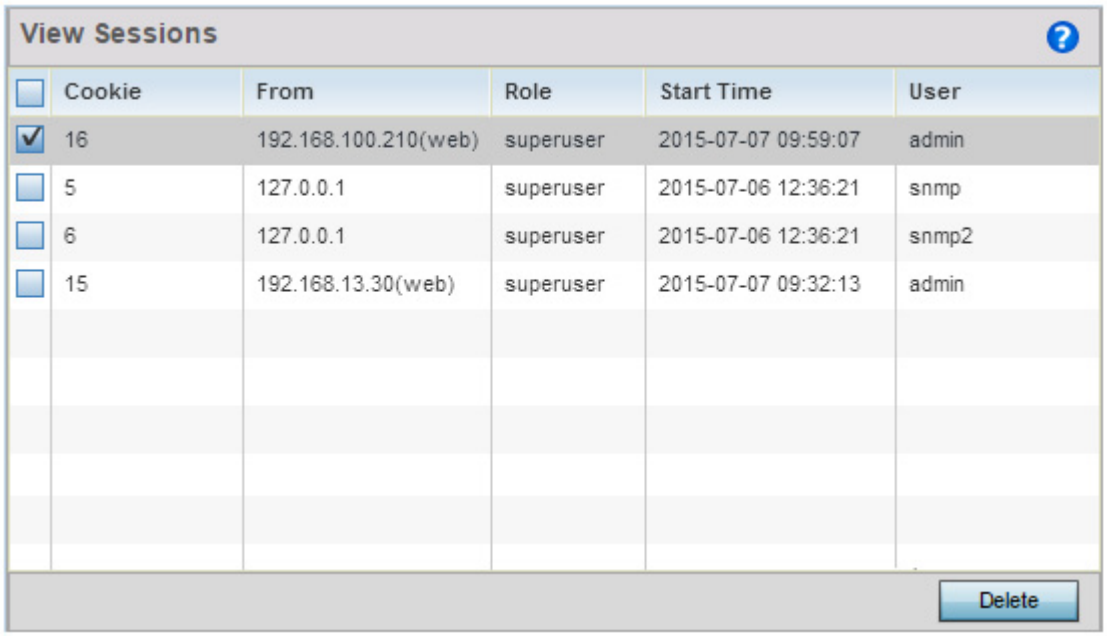



**Figure 421: Advanced - View Sessions screen**

3 Refer to the following table for more information on the fields displayed in this screen:

| | |
|---|---|
| Cookie | Displays the number of cookies created by this session. |
| From | Displays the IP address of the device/process initiating this session. |
| Role | Displays the role assigned to the user name as displayed in the User column. |
| Start Time | Displays the start time of this session. This is the time at which the user successfully created this session. |
| User | Displays the user name of the account used to initiate this session. |

4 To remove a listed session, select the check box before session, then select **Delete**.

# 13 Operations



The functions supported within the Operations menu allow the administration of firmware, configuration files and certificates for managed devices.

A certificate links identity information with a public key enclosed in the certificate. Device certificates can be imported and exported to a secure remote location for archive and retrieval as they are required for application to other managed devices.

*Self Monitoring At Run Time RF Management* (Smart RF) is an innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization and radio performance improvements. The Smart RF functionality scans the managed network to determine the best channel and transmit power for each managed access point radio.

For more information, refer to the following:

- Device Operations on page 873
- Certificates on page 891
- Smart RF on page 908

## Device Operations

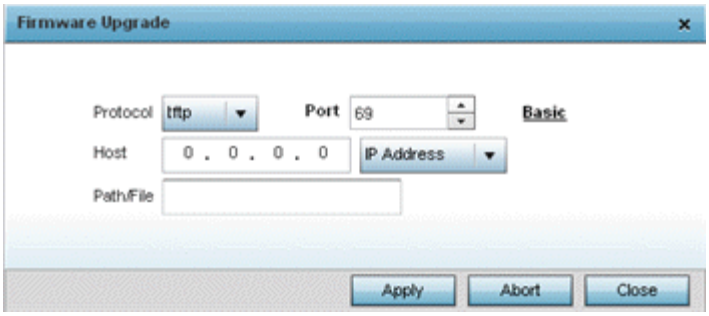
Updated controller, service platform and access point firmware and configuration files are periodically updated and released to the Support Web site. If your device's firmware is older than the version on the Web site, consider updating to the latest version for full feature functionality and optimal controller utilization. Additionally, selected devices can either have a primary or secondary firmware image applied or fallback to a selected firmware image if an error occurs in the update process.

### Upgrading Device Firmware

Controllers, service platforms and access points has can conduct firmware updates for their managed or peer devices. access points can only update the firmware of peer access point models of the same type.

To update the firmware of a managed device:

1 Go to **Operations → Devices**.
2 Expand the **System** node and select an **RF Domain** from those listed.
3 Expand the **RF Domain** node and select a device. The selected device's Summary page displays by default.
4 Click the **Firmware Upgrade** button to start firmware upgrade.




By default, the Firmware Upgrade screen displays the tftp server parameters for the target device firmware file.

5 Enter the complete path to the firmware file for the target controller, service platform or access point in the Path/File field.

6 Provide the following information to accurately define the location of the target firmware file:

| | |
|---|---|
| Protocol | Select the connection protocol used for updating device firmware. Available options include:<br>*tftp*<br>*ftp*<br>*sftp*<br>*http*<br>*cf*<br>*usb1-4* |
| Port | Use the spinner control or manually enter the value to define the port used for firmware updates. This option is not valid for *cf* and *usb1-4*. |
| IP Address | Enter IP address of the server used to update the firmware. This option is not valid for *cf* and *usb1-4*. |
| Hostname | Provide the hostname of the server used to update the firmware. This option is not valid for *cf* and *usb1-4*. |
| User Name | Define the user name used to access either a *FTP* or *SFTP* server. |
| Password | Specify the password for the user account to access a *FTP* or a *SFTP* server. |
| Path / File | Specify the path to the firmware file. Enter the complete relative path to the file on the server. |

7 Select Apply to start the firmware update. Select Abort to terminate an in process firmware update. Select Close to close the upgrade pop up screen. The upgrade continues in the background.

## Adopted Device Upgrades

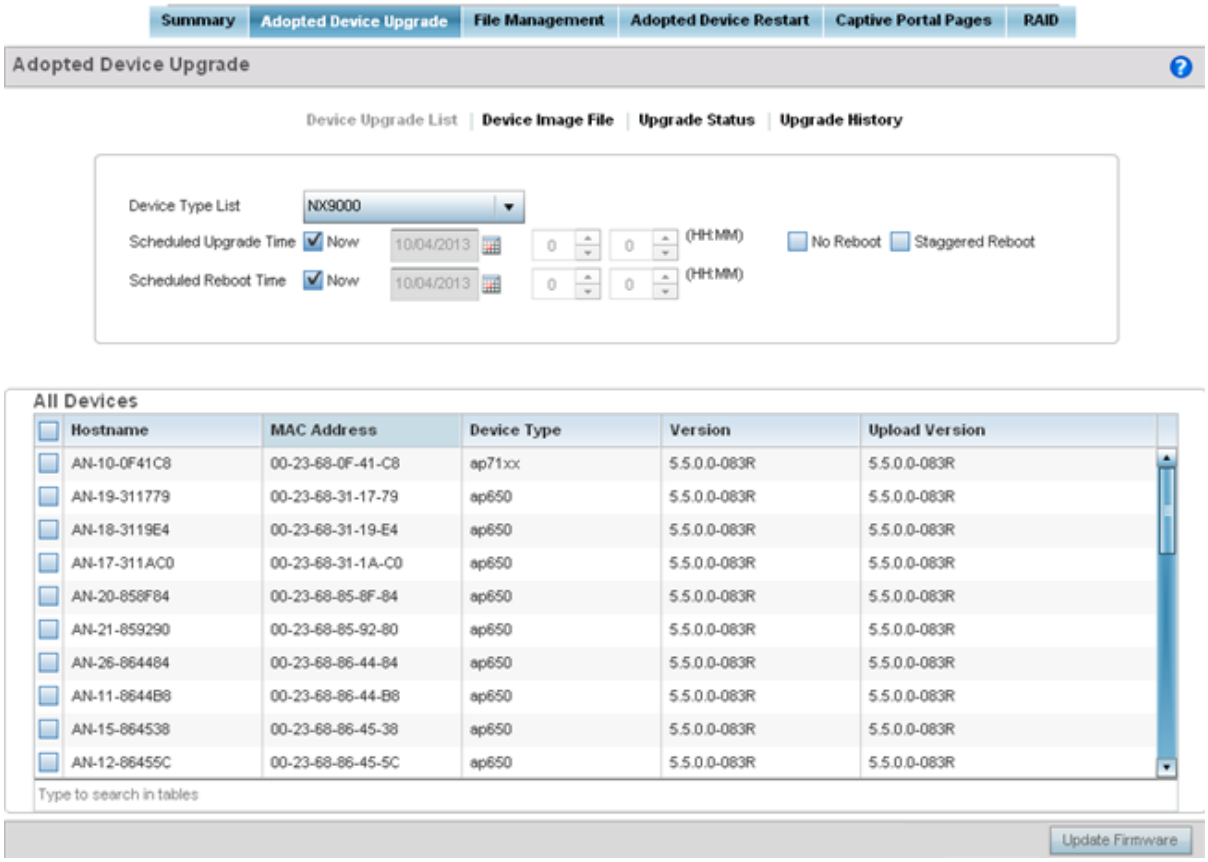
An administrator can designate controllers, service platforms or access points as RF Domain managers capable of receiving firmware files from the NOC (NX7500 or NX9000 series service platforms) then provisioning other devices within their same RF Domain. Controllers, service platforms and access points can now all update the firmware of different device models within their RF Domain. However, firmware updates cannot be made simultaneously to devices in different site deployments.

### *Device Upgrade List*

1 Ensure Devices is selected from the Operations menu on the top, left-hand, side of the screen.

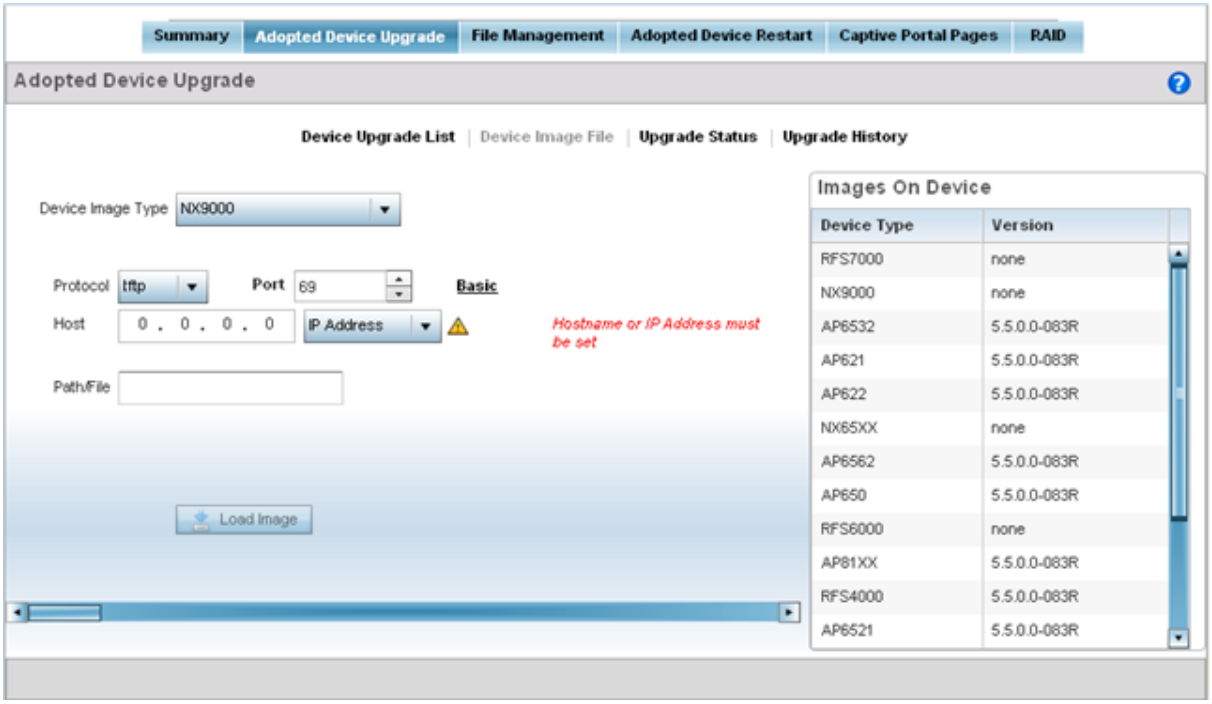
2 Expand the System node, select a RF Domain and one of its member devices.

3 Select **Adopted Device Upgrade**. The screen displays with the **Device Upgrade List** selected by default.




4 Select the controller, service platform or access point model from the **Device Type List** drop-down menu. This is the device model used to provision firmware to the devices selected within the All Devices table below. Selecting **All** makes each controller, service platform and access point model images available for updates on those specific models.

5 Select **Device Image File**. Use this screen to select device image types for firmware updates and set the transfer protocol used for staging the firmware to the device itself prior to its update.




6 Select the **Basic** link to enter a URL pointing to the location of the controller, service platform or access point image files for the device update(s).

7 Selecting **Advanced** lists additional options for the device's firmware image file location:

| | |
|---|---|
| Protocol | Select the protocol for device firmware file management and transfer. Available options include:<br>*tftp*<br>*ftp*<br>*sftp*<br>*http*<br>*cf* |
| Port | Designate the port for transferring the firmware files used in the upgrade operation. Enter the port number directly or use the spinner control. |
| Host | Specify a numerical IP address or textual Hostname of the resource used to transfer files to the *devices* designated for a firmware update. |
| Path / File | Define the path to the file on the file repository resource. Enter the complete relative path to the file. |

8 Select the **Load Image** button to upload the device firmware.

The firmware image is loaded to the flash/upgrade directory (not the flash/cache directory). If the NOC pushes the image, then it is loaded to flash/cache/upgrade.

### *Device Image File*

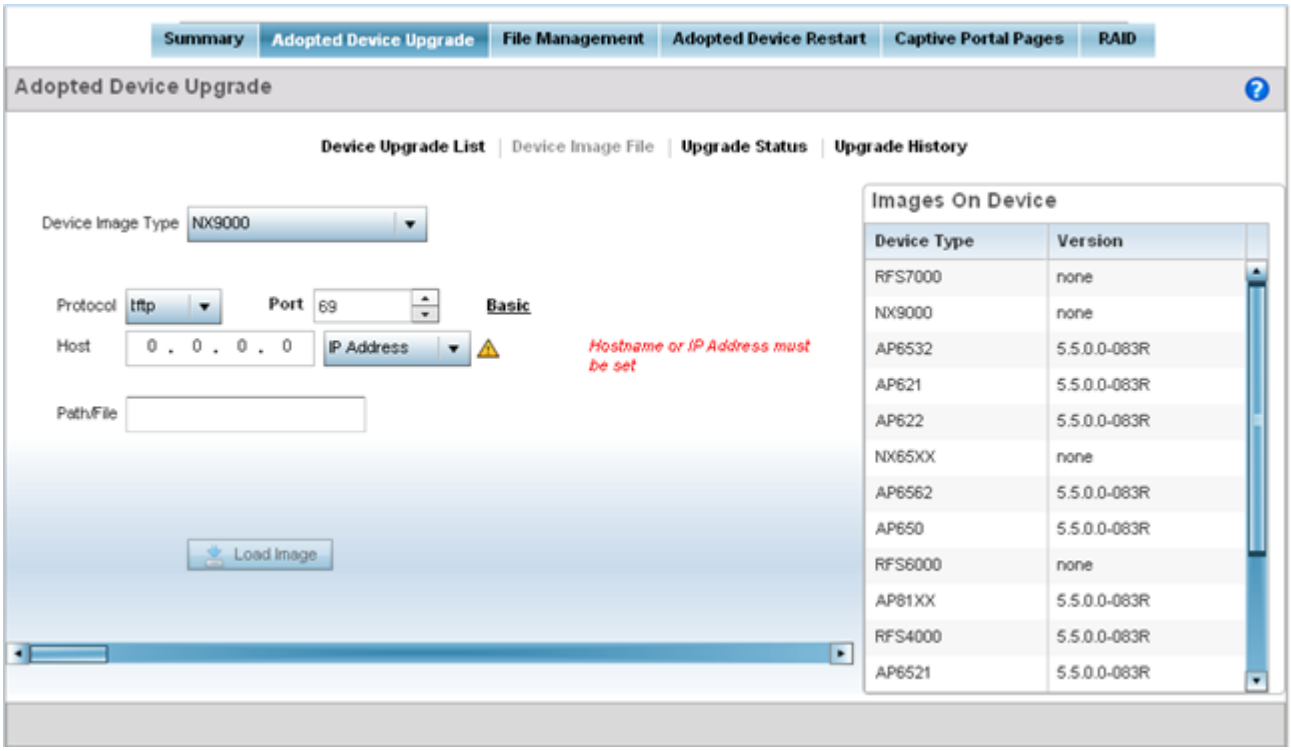
Use the **Device Image File** screen to select device image types for firmware updates and set the transfer protocol used for staging the firmware to the device itself prior to its update.

To define an upgrade configuration for a controller, service platform or access point:

1 Select **Operations**.

2 Ensure **Devices** is selected from the Operations menu on the top, left-hand, side of the screen.

3 Expand the System node, select a RF Domain and one of its member devices.
4 Select the Adopted Device Upgrade tab.
5 Select Device Image File.




6 Select the controller, service platform or access point model from the Device Type List drop-down menu. This is the device model used to provision firmware to the devices selected within the All Devices table below. Selecting All makes each controller, service platform and access point model images available for updates on those specific models.
7 Select the Basic link to enter a URL pointing to the location of the controller, service platform or access point image files for the device update(s).
8 Selecting Advanced lists additional options for the device's firmware image file location:

| | |
|---|---|
| Protocol | Select the protocol for device firmware file management and transfer. Available options include:<br>*tftp*<br>*ftp*<br>*sftp*<br>*http*<br>*cf* |
| Port | Designate the port for transferring the firmware files used in the upgrade operation. Enter the port number directly or use the spinner control. |
| Host | Specify a numerical IP address or textual Hostname of the resource used to transfer files to the *devices d*esignated for a firmware update. |
| Path / File | Define the path to the file on the file repository resource. Enter the complete relative path to the file. |

9 Select the Load Image button to upload the device firmware.

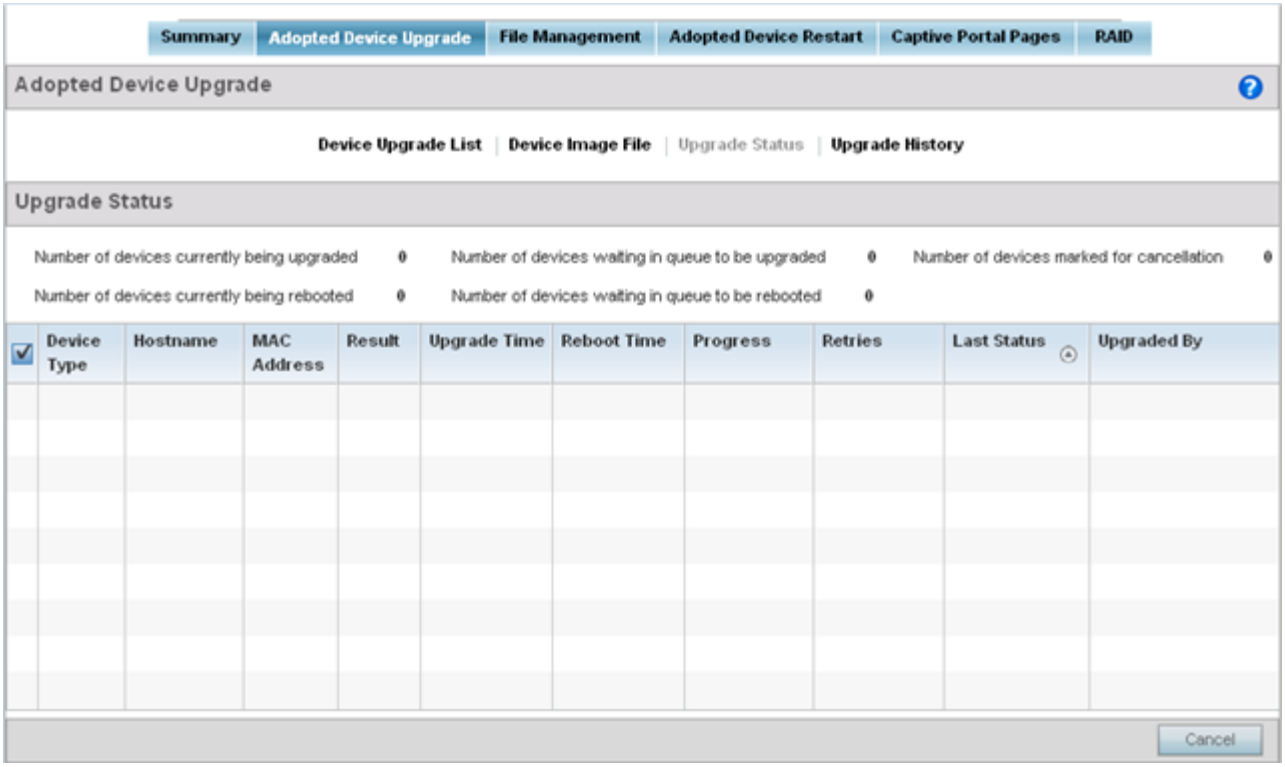
The firmware image is loaded to the flash/upgrade directory (not the flash/cache directory). If the NOC pushes the image, then it is loaded to flash/cache/upgrade.

*Upgrade Status*

Once an upgrade operation has been started or schedules, an administrator can assess whether the upgrade was successful, the number of times the operation was attempted before completed and the upgraded device's current status.

To assess the administration, scheduling and progress of device firmware updates:

1 Select Operations.
2 Ensure Devices is selected from the Operations menu on the top, left-hand, side of the screen.
3 Expand the System node, select a RF Domain and one of its member devices.
4 Select the Adopted Device Upgrade tab.
5 Select Upgrade Status.




6 Refer to the Upgrade Status field to assess the completion of in-progress upgrades.

| | |
|---|---|
| Number of devices currently being upgraded | Lists the number of firmware upgrades currently in-progress and downloading for selected devices. Once the device has the image it requires a reboot to implement the firmware image. |
| Number of devices currently being booted | Lists the number devices currently booting after receiving an upgrade image. The reboot is required to implement the new image and renders the device offline during that period. Using the *Device Upgrade List*, reboots can be staggered or placed on hold to ensure device remains in service. |
| Number of devices waiting in queue to be upgraded | Lists the number of devices waiting to receive a firmware image from their provisioning controller, service platform or access point. Each device can have its own upgrade time defined, so the upgrade queue could be staggered. |

| | |
|---|---|
| Number of devices waiting in queue to be upgraded | Lists the number of devices waiting to reboot before actively utilizing its upgraded image. The *Device Upgrade List* list allows an administrator to disable or stagger a reboot time, so device reboots may not occur immediately after an upgrade. The reboot operation renders the device offline until completed so reboots can scheduled for periods of reduced load |
| Number of devices marked for cancelation | Lists the number of upgrades that have been manually canceled during the upgrade operation. |

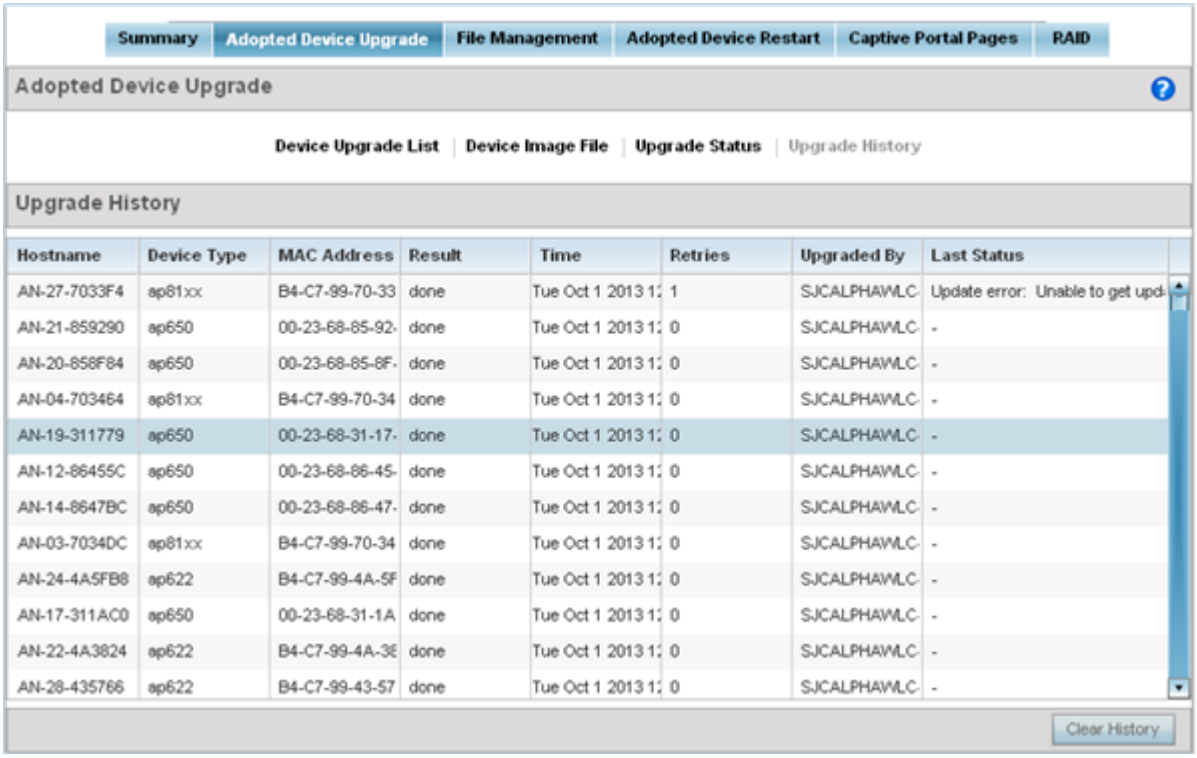
7 Refer to the following status reported for each current or scheduled upgrade operation:

| | |
|---|---|
| Device Type | Displays the model number of devices pending an upgrade. Each listed device is provisioned an image file unique to that model. |
| Hostname | Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades. |
| MAC Address | Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades. |
| Result | Lists the state of an upgrade operation (*downloading, waiting for a reboot* etc.). |
| Upgrade Time | Displays whether an upgrade is immediate or set by an administrator for a specific time. Staggering upgrades is helpful to ensure a sufficient number of devices remain in service at any given time while others are upgrading. |
| Reboot Time | Displays whether a reboot is immediate or time set by an administrator for a specific time. Reboots render the device offline, so planning reboots carefully is central to ensuring a sufficient number of devices remain in service. |
| Progress | Lists the number of specific device types currently upgrading. |
| Retries | Displays the number of retries, if any, needed for an in-progress firmware upgrade operation. |
| Last Status | Lists the last reported upgrade and reboot status of each listed in progress or planned upgrade operation. |
| Upgraded By | Lists the model of the controller, service platform or access point RF Domain manager that's provisioning an image to a listed device. |

8 Optionally select Cancel (from the lower, right-hand corner of the screen) to cancel the upgrade of devices under the selected RF Domain. The Cancel button is enabled only if there are device undergoing upgrade and they're are selected for cancelation.

9 Select Upgrade History.

Once an upgrade operation has completed, an administrator can assess whether the upgrade was successful, the number of times the operation was attempted before completed and any errors encountered while upgrading.




10 Refer to the following **Upgrade History** status:

| | |
|---|---|
| Hostname | Displays the administrator assigned Hostname for each listed controller, service platform or access point that's received an update. |
| Device Type | Displays the controller, service platform or access point model upgraded by a firmware update operation. |
| MAC Address | Displays the device *Media Access Control* (MAC) or hardware address for a device that's received an update. |
| Result | Displays the upgrade result for each listed device. |
| Time | Displays the time and date of the last status received from an upgraded device. |
| Retries | Displays the number of retries, if any, needed for the firmware upgrade operation. |
| Upgraded By | Displays the administrator credentials responsible for initiating each listed upgrade operation. |
| Last Status | Displays the last status update received for devices that have been upgraded. |

11 Select the **Clear History** button to clear the current update information for each listed device and begin new data collections.

### *Device Upgrade History*

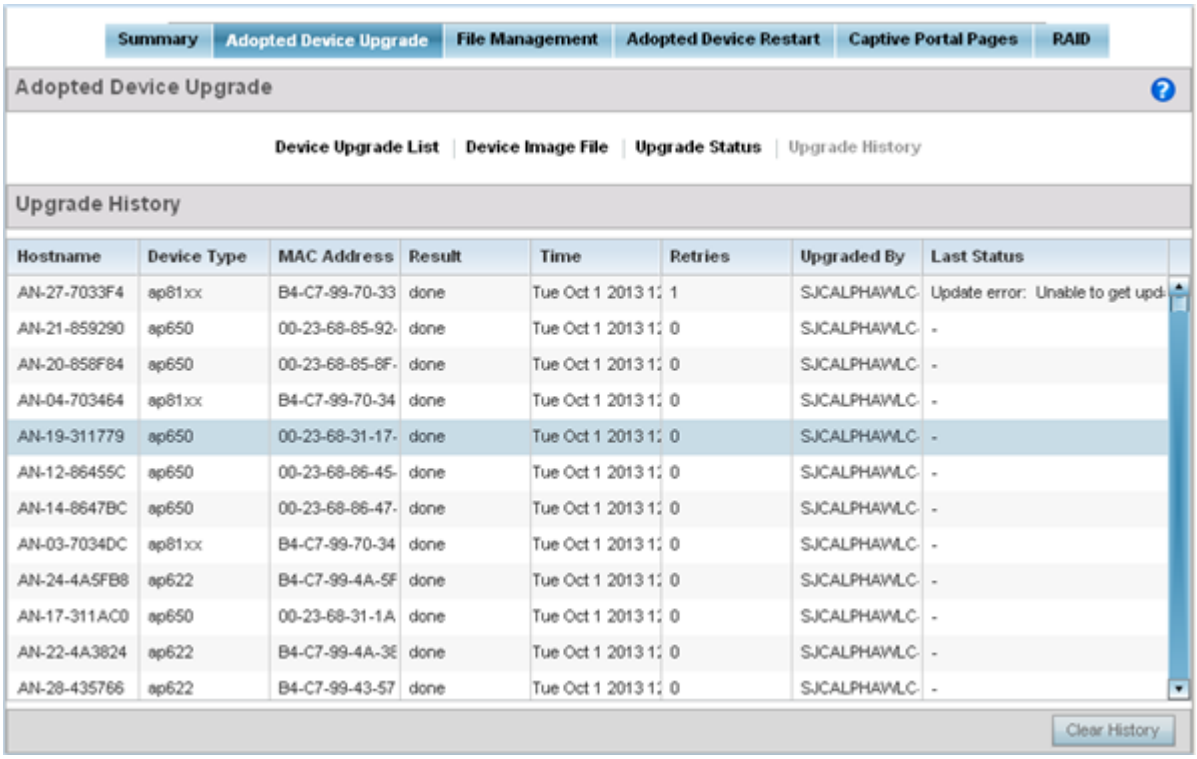
Once an upgrade operation has completed, an administrator can assess whether the upgrade was successful, the number of times the operation was attempted before completed and any errors encountered while upgrading.

To assess the administration, scheduling and progress of device firmware updates:

1 Select **Operations**.

2 Ensure **Devices** is selected from the Operations menu on the top, left-hand, side of the screen.

3 Expand the System node, select a RF Domain and one of its member devices.
4 Select the Adopted Device Upgrade tab.
5 Select Upgrade History.




6 Refer to the following Upgrade History status:

| | |
|---|---|
| Hostname | Displays the administrator assigned Hostname for each listed controller, service platform or access point that's received an update. |
| Device Type | Displays the controller, service platform or access point model upgraded by a firmware update operation. |
| MAC Address | Displays the device *Media Access Control* (MAC) or hardware address for a device that's received an update. |
| Result | Displays the upgrade result for each listed device. |
| Time | Displays the time and date of the last status received from an upgraded device. |
| Retries | Displays the number of retries, if any, needed for the firmware upgrade operation. |
| Upgraded By | Displays the administrator credentials responsible for initiating each listed upgrade operation. |
| Last Status | Displays the last status update received for devices that have been upgraded. |

7 Select the Clear History button to clear the current update information for each listed device and begin new data collections.

## Using the File Management Browser

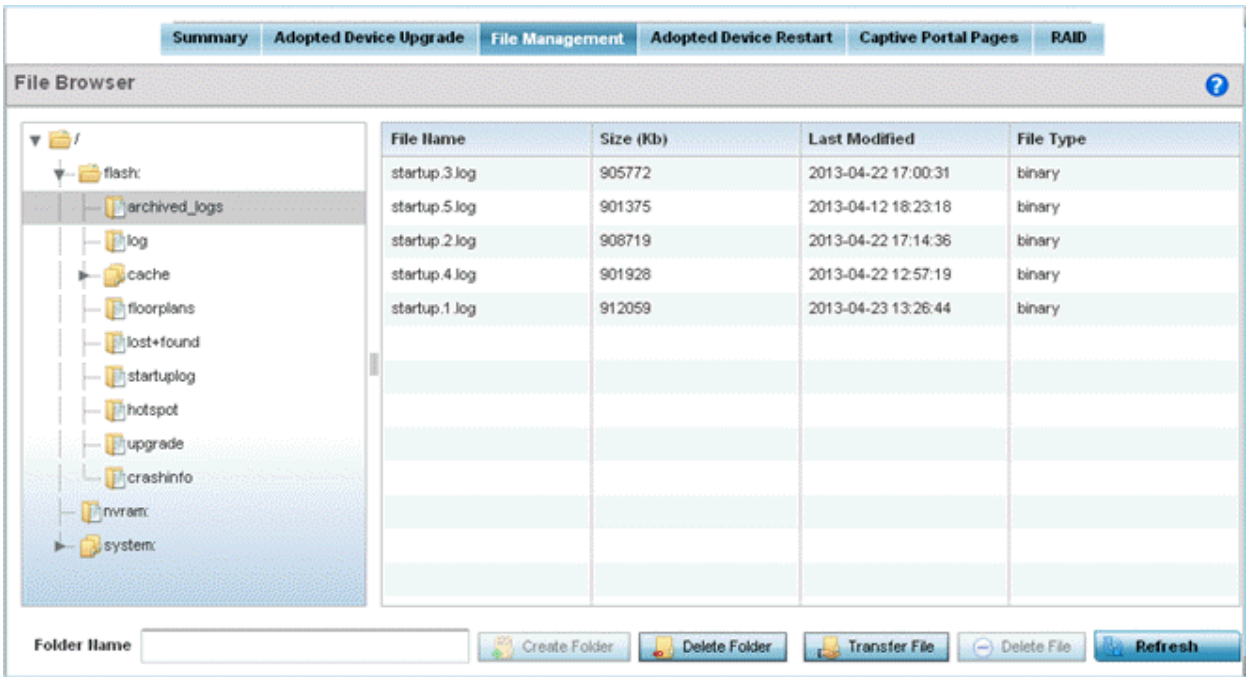
Controllers, service platforms and access points can utilize a File Browser allowing an administrator to review the files residing on a internal or external memory resource. Directories can be created and maintained for each File Browser location and folders and files can be moved and deleted as needed.

**Note**

The **File Management** tab is not available at the RF Domain level of the UI's hierarchal tree. A RF Domain must be selected and expanded to display the RF Domain's member devices. Once expanded, selected a RF Domain member device to ensure the File Management UI option is available.

To administer files for managed devices and memory resources:

1 Select the **Operations** > **Devices** > **File Management.**




2 Refer to the following to determine whether a file needs to be deleted or included in a new folder for the selected internal (flash, system, nvram) or external (cf, USB1 -4) memory resource. The following display for each available memory resource:

| | |
|---|---|
| File Name | Displays the name of the file residing on the selected *flash*, *system*, *nvram* or *usb1-4* location. The name cannot be modified from this location. |
| Size (Kb) | Displays the size of the file in kb. Use this information to help determine whether the file should be moved or deleted. |
| Last Modified | Lists a timestamp for the last time each listed file was modified. Use this information to determine the file's relevance or whether it should be deleted. |
| File Type | Displays the type for each file including binary, text or empty. |

3 If needed, use the **Create Folder** utility to create a folder that servers as a directory for some or all of the files for a selected memory resource.

4 Select Transfer File to invoke a subscreen where the local or server file source and target (destination) are defined as well as the file transfer protocol and external destination location or resource.

5 Optionally, use the Delete Folder or Delete File buttons to remove a folder or file from within the current memory resource.

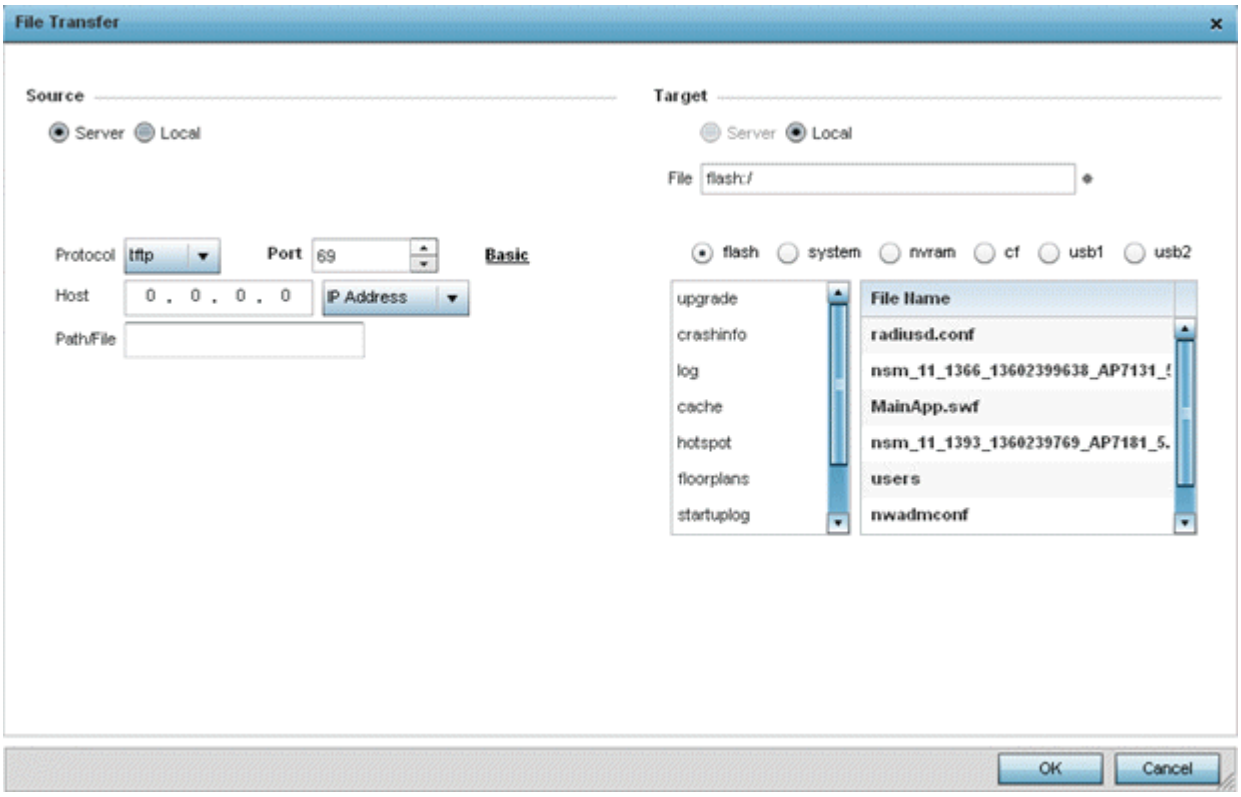
*Managing File Transfers*

Controllers and service platforms can administer files on managed devices. Transfer files from a device to this controller, to a remote server or from a remote server to the controller. An administrator can transfer logs, configurations and crash dumps.

To administer files for managed devices:

1 Go to **Operations → Devices → File Management**.

2 Select the Transfer File button.




3 Set the following file management source and target directions and the configuration parameters of the required file management activity:

| | |
|---|---|
| Source | Select the source of the file transfer.<br>Select *Server* to indicate the source of the file is a remote server external to the controller or access point.<br>Select *Local* to indicate the source of the file is the local device. |
| File | If the source is *Local*, enter the name of the file to be transferred. |

| | |
|---|---|
| Protocol | Select the protocol for file management. Available options include:<br>•*tftp*<br>•*ftp*<br>•*sftp*<br>•*http*<br>•*cf*<br>•*usb1-4*<br>This parameter is required only when *Server* is selected as the Source. |
| Port | Specify the physical port for transferring files. This option is not available for *cf* and *usb1-4*. Enter the port number directly or use the spinner control.<br>This parameter is required only when *Server* is selected as the Source. |
| Host | If needed, specify a hostname or numeric IP address of the serve transferring the file. This option is not valid for cf and usb1-4. If a hostname is provided, an IP Address is not needed.<br>This field is only available when Server is selected in the From field. |
| User Name | Provide a user name to access a FTP or a SFTP server.<br>This parameter is required only when *Server* is selected as the Source, and the selected protocol is *ftp* or *sftp*. |
| Password | Provide a password to access the FTP or SFTP server.<br>This parameter is required only when *Server* is selected as the Source, and the selected protocol is *ftp* or *sftp*. |
| Path / File | Define the path to the file on the server. Enter the complete relative path to the file.<br>This parameter is required only when *Server* is selected as the Source. |
| Target | Select the target destination to transfer the file.<br>•Select *Server* if the destination is a remote server, provide a URL to the location of the server resource or select Advanced and provide the same network address information described above.<br>•Select *Local* if the destination is the controller, service platform or access point. |

4 Select **Copy** to begin the file transfer. Selecting **Reset** reverts the screen to its last saved configuration.

## Crypto CMP Certificate

Certificate Management Protocol (CMP) is an Internet protocol to obtain and manage digital certificates in a Public Key Infrastructure (PKI) network. A Certificate Authority (CA) issues the certificates using the defined CMP.

Using CMP, a device can communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.

The CMP client on the controller, service platform or Access Point triggers a request for the configured CMS CA server. Once the certificate is validated and confirmed from the CA server it is saved on the device and becomes part of the trustpoint. During the creation of the CMP policy the trustpoint is assigned a name and client information. An administrator can use a manually created trustpoint for one service (like HTTPs) and use the CMP generated trustpoint for RADIUS EAP certificate based authentication.

Use the Crypto CMP Certificate menu item to manage these certificates:

1 Refer to the following for more information on Crypto CMP Certificates:

:

| | |
|---|---|
| Hostname | Lists the administrator assigned hostname of the CMP resource requesting a certificate renewal from the CMP CA server. |
| MAC Address | Lists the hardware encoded MAC address of the CMP server resource. |
| Trust Point Name | Trust Point Name Lists the 32 character maximum name assigned to the target trustpoint. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. |
| Trust Point Valid Until | The expiration of the CMP certificate is checked once a day. When a certificate is about to expire a certificate renewal can initiated with the server via an existing IPsec tunnel. If the tunnel is not established, the CMP renewal request is not sent. |

2 Select **Trigger Certificate Renewal** to begin update the credentials of the certificate. If a renewal succeeds, the newly obtained certificate overwrites an existing certificate. If the renewal fails, an error is logged.

3 Select **Refresh** to update the screen to the last saved configuration.

## Restarting Adopted Devices

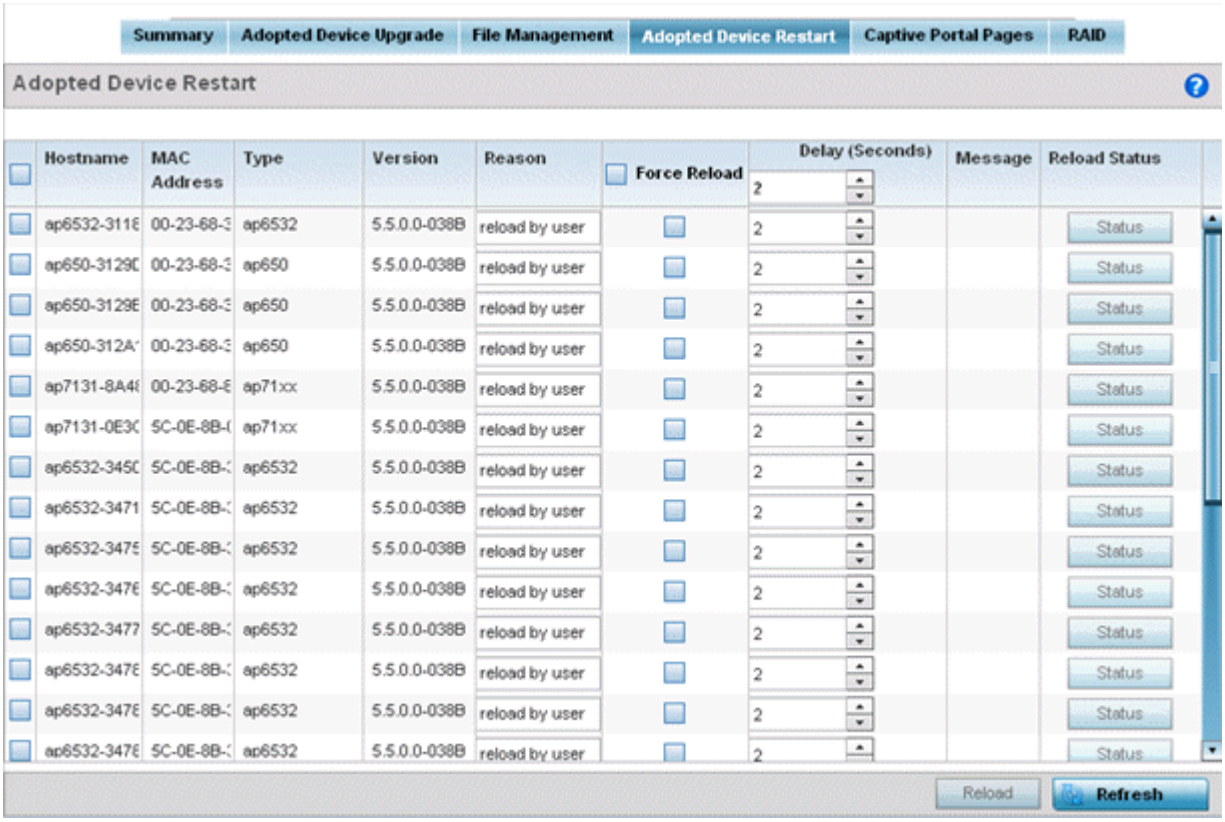
Controllers and service platforms can restart their adopted access points as needed for firmware upgrades or other administrative activities. access points set in Controller AP mode also have the ability to restart adopted peer model access points.

Note

The Adopted Device Restart tab is not available at the RF Domain level of the UI's hierarchal tree. A RF Domain must be selected and expanded to display the RF Domain's member devices. Once expanded, selected a RF Domain member device to ensure the Adopted Device Restart option is available.

To restart one or mode adopted access points:

1 Select the Operations > Devices > Adopted AP Restart.




2 The Adopted AP Restart table displays the following information for each Adopted AP:

| | |
|---|---|
| Hostname | Displays the administrator assigned hostname for each known access point. |
| MAC Address | Displays the factory assigned *Media Access Control* (MAC) or hardware address for each known access point. |
| Type | Displays the access point model number for each adopted access point. |
| Version | Displays the current firmware version for each adopted access point. |
| Reason | Lists the administrator defined reason an adopted device has been queued for a restart. |

3 To restart one or more access points, select the checkbox to the left of each AP and set the following options:

| | |
|---|---|
| Force Reload | To force a reload of an access point (or multiple access points), select the *Force Reload* checkbox next to the target AP. |
| Delay (Seconds) | Specify the amount of time, in seconds, before the access point restart is executed. Setting a delay time is recommended when an access point load cannot be assumed by a neighbor AP until a known time in the near future. |
| Message | Displays a message relating to the access point's current adoption. |
| Reload Status | Click the *Reload Status* button next to each adopted access point to display each device's current status information. |

## Captive Portal Configuration

For information moving captive portal configurations to managed access points and making captive portals available to requesting clients, see:

- AP Upload
- CP Page Image File
- Status

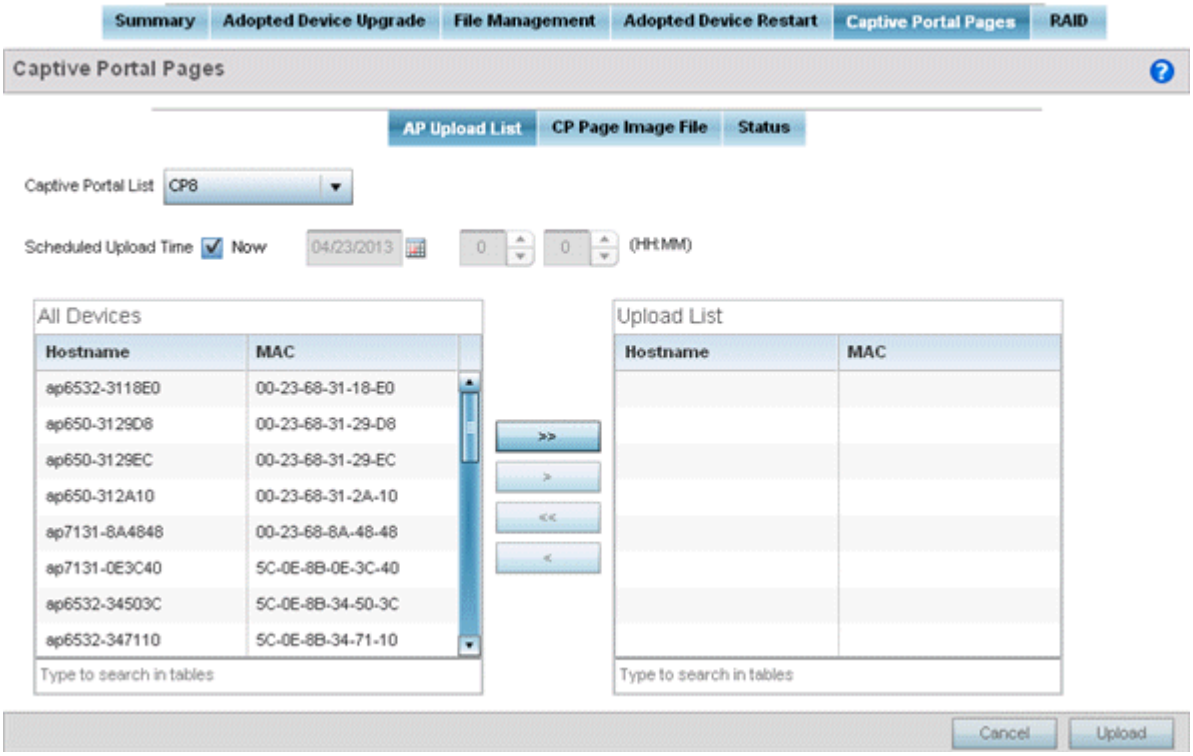
### *AP Upload List*

Use the **AP Upload List** to provide connected access points with specific captive portal configurations so they can successfully provision login, welcome and condition pages to requesting clients attempting to access the wireless network using a captive portal.

To upload captive portal pages to connected access points:

1 Select the **Operations** menu item.

2 Select **Devices** and select the **Captive Portal Pages** tab. The **AP Upload List** tab displays by default.



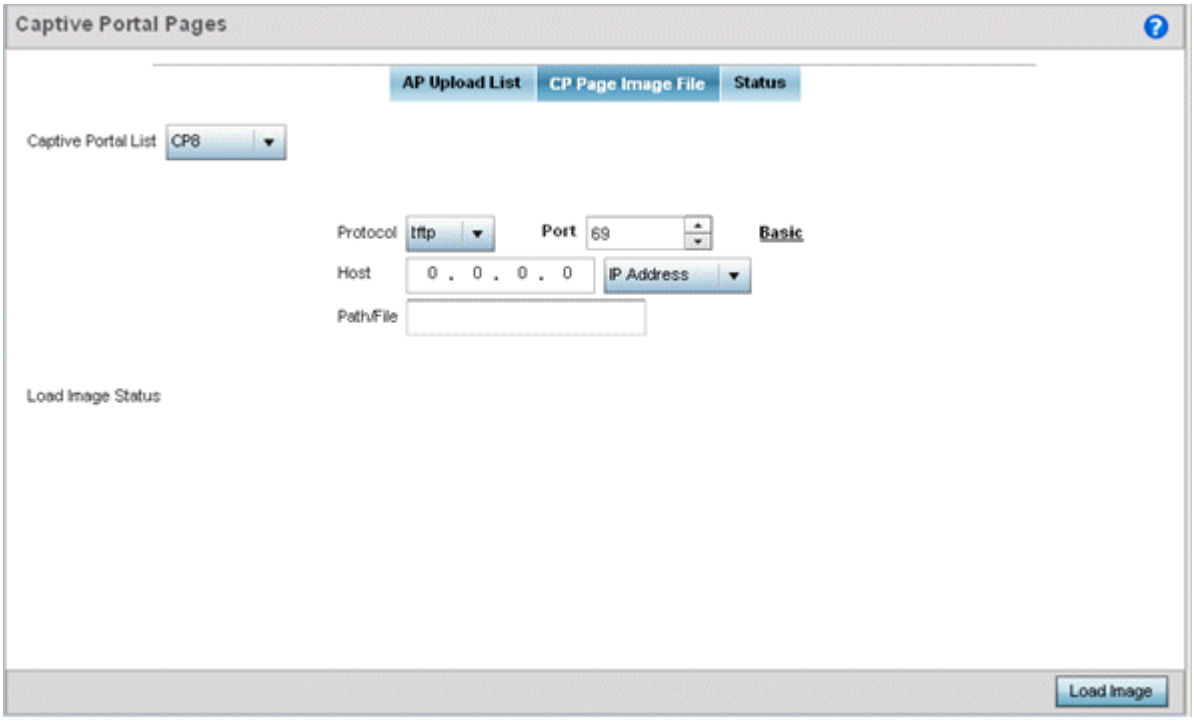

3 Use the **Captive Portal List** drop-down menu to select an existing captive portal configuration to upload to an access point and display to requesting client devices as they login and adhere to the terms required for captive portal access.

### *CP Page Image File*

Use the **CP Pages Image File** screen to set the way managed access points receive captive portal images files required to provision captive portal access to requesting clients. Captive portal image files are the login, welcome and conditions pages specifically.

To set the captive portal for upload and define the transfer configuration:

1 Got to **Operations → Devices → System**.
2 Expand one of the **RF Domains** listed within the System node, and select a target device.
3 Go to the **Captive_Portal_Distribute_Pages → CP Pages Image File** tab.




4 Set the following Captive Portal page upload settings:

| | |
|---|---|
| Captive Portal List | Use the drop-down menu to select an existing policy. This policy contains the image (or set of login and conditions pages) requesting clients will navigate and complete before granted access to the network using the unique permissions of the captive portal. |
| Protocol | Define the protocol (transfer medium) used to forward the image files to the access points provisioning captive portal files to requesting clients. Available options include *ftp, http, tftp* and *sftp*. A protocol parameter is required only when Server is selected as the Source and the Advanced option is used. |
| Host | If needed, specify a Hostname or numeric IP address of the server transferring the file. If a hostname is provided, an *IP Address* is not needed. This field is only available when Server is selected in the *From* field. |
| Port | Specify the port for transferring files. Enter the port number directly or use the spinner control.. |
| User Name | Provide a user name to access the FTP or SFTP server. This parameter is required only when the selected protocol is ftp or sftp. |
| Password | Provide the password for the user name used to log in to the FTP/SFTP server. Only required when the protocol is ftp or sftp. |
| Path/File | Define the path to the file on the server. Enter the complete relative path to the file. |

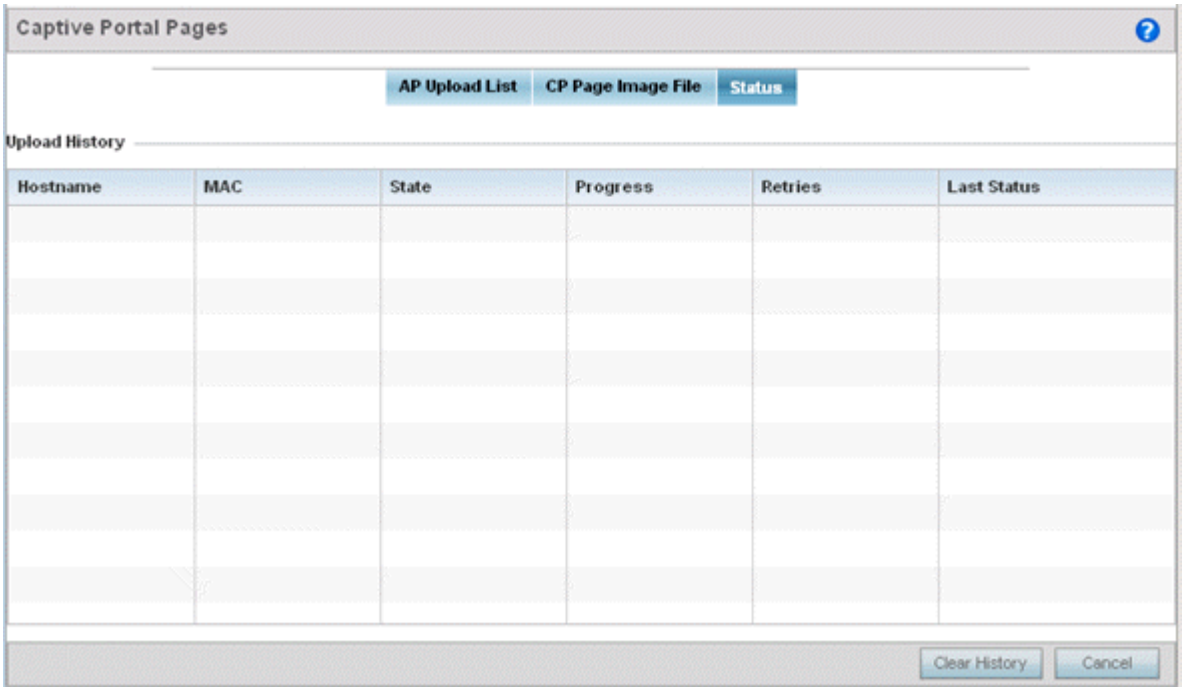
5 Select Load Image to upload the image file. Optionally, refer to the Load Image Status field to review the status of the current upload.

*Status*

Use the **Status** screen to review those devices targeted for captive portal image uploads, their operational state and image upload completion status:

To assess the progress and completion status of captive portal image uploads:

1 Select the **Operations** menu item.
2 Select **Devices** and select the **Captive Portal Pages** tab.
3 Select the **Status** tab.




4 Refer to the following:

| | |
|---|---|
| Hostname | Displays the administrator defined hostname for the device receiving the captive portal page upload. |
| MAC | Displays the hardware encoded *Media Access Control* (MAC) address of the unit performing the captive portal page upload. |
| State | Displays the target device's current operational state within the controller or service platform managed network. |
| Progress | Displays the current upload progress for each captive portal page upload. |
| Retries | Lists the number of retries needed to upload the captive portal files to each listed device. |
| Last Status | Displays the last known status of the captive portal page upload to each listed device. |

5 Select **Clear History** to clear the history displayed in the Status tab and begin new data collections.

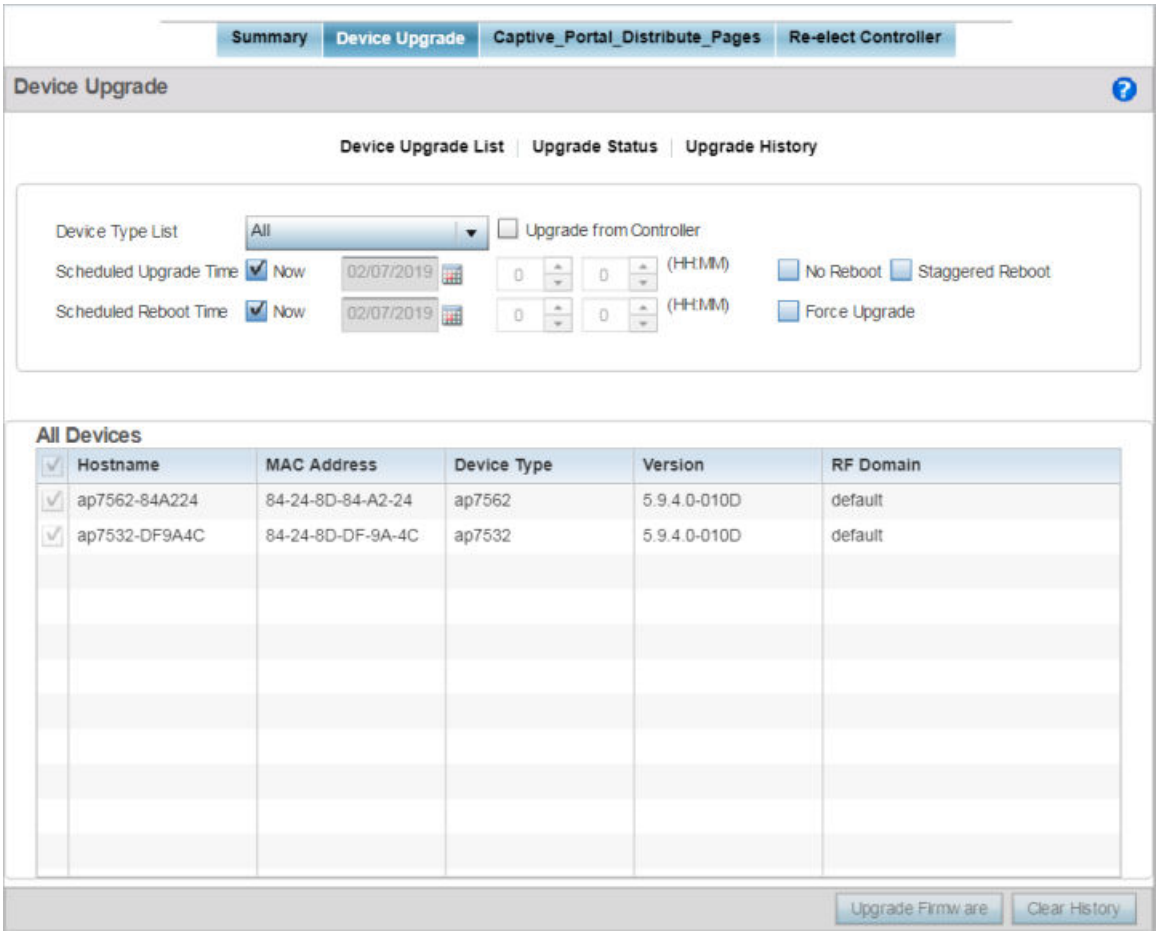
## RF Domain - Device Upgrade Operation

You can configure device upgrade operation at the RF Domain level. RF Domain upgrades happen through the RF Domain manager. The RF Domain manager, requests and receives the firmware from the

controller and upgrades RF Domain member devices. Therefore, prior to configuring device upgrade on the RF Domain, ensure the Controller is upgraded to the latest firmware. For more information, see Upgrading Device Firmware on page 873.

To configure RF Domain level device upgrade:

1 Go to **Operations → Devices**.
2 Expand the **System** node and selected a member **RF Domain**.
3 Select the **Device Upgrade** tab.




4 Select the **Device Upgrade List** tab, if not selected by default.
5 Use the Device Type List drop-down menu to select the type of device to be upgraded. This is the device model used to provision firmware to the devices selected within the All Devices table below.

   Select the **All** option to initiate upgrade of all devices within the selected RF Domain. If you select this option, the All Devices table is disabled.
6 Select the **Upgrade from Controller** checkbox to initiate upgrade through the controller to which the selected device is adopted.
7 Use the Scheduled Upgrade Time and Scheduled Reboot Time options to schedule the upgrade at a latter time.

   By default, both the Scheduled Upgrade Time and Scheduled Reboot Time options are set to **Now**, which initiates immediate upgrade.

# Certificates

A certificate links identity information with a public key enclosed in the certificate.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its Trusted Root Library so it can trust certificates *signed* by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a client to access managed resources, if properly configured. A RSA key pair must be generated on the client. The public portion of the key pair resides locally with the controller, service platform or access point, while the private portion remains on a secure local area of the client.

For more information on the certification activities supported, refer to the following:

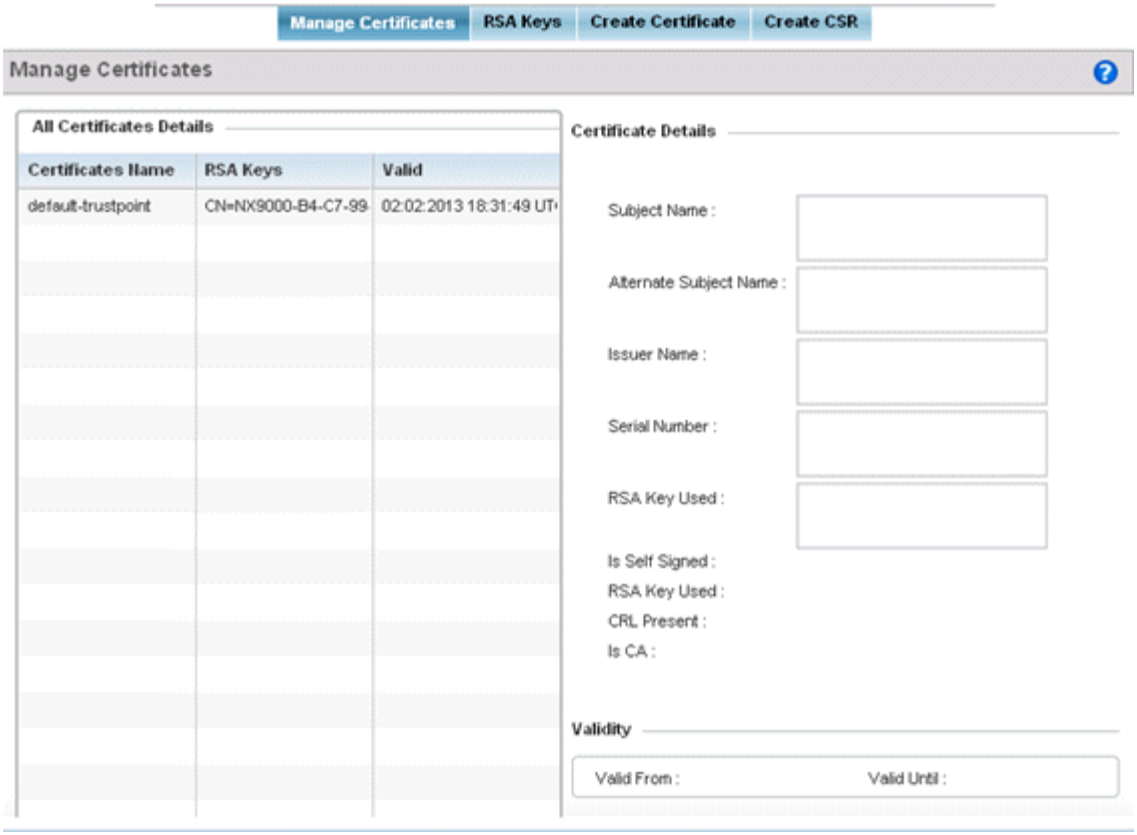

- Certificate Management on page 891
- RSA Key Management on page 900
- Certificate Creation on page 904
- Generating a Certificate Signing Request on page 906


## Certificate Management

If not wanting to use an existing key or certificate, a *stored* certificate can be leveraged from a peer controller, service platform or access point. Device certificates can be imported and exported to a secure remote location for archive and retrieval as they are required for application to other managed devices.

To configure trustpoints for use with certificates:

1 Select **Operations** > **Manage Certificates.**
2 Select a device from amongst those displayed in either the RF Domain or Network panes on the left-hand side of the screen.




The **Manage Certificates** screen displays for the selected MAC address.

3 Select a device from amongst those displayed to review its certificate.

4 Refer to the **All Certificate Details** to review the certificate's properties, self-signed credentials, validity period and CA information.

5 To import a certificate to the controller or service platform, select the **Import** button from the bottom of the Manage Certificates screen.

An **Import New Trustpoint** screen displays where CA certificates, CRLs and signed certificates can optionally be imported to the controller or service platform once the network credentials of the file transfer have been defined.

### *Import Certificates and Trustpoints*

A certificate links identity information with a public key enclosed in the certificate. Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

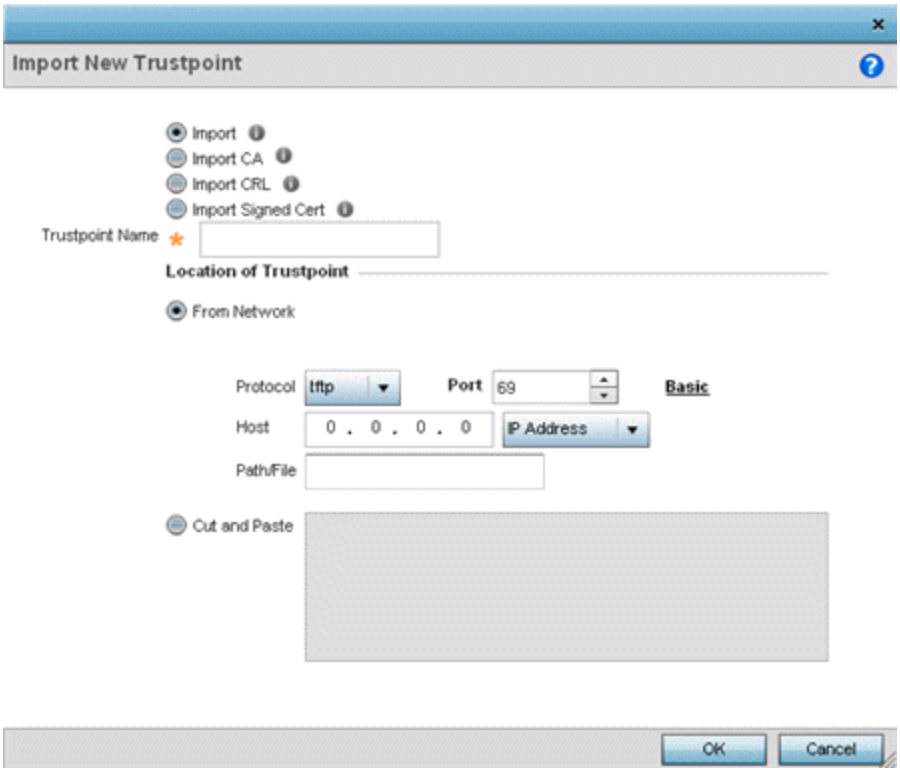
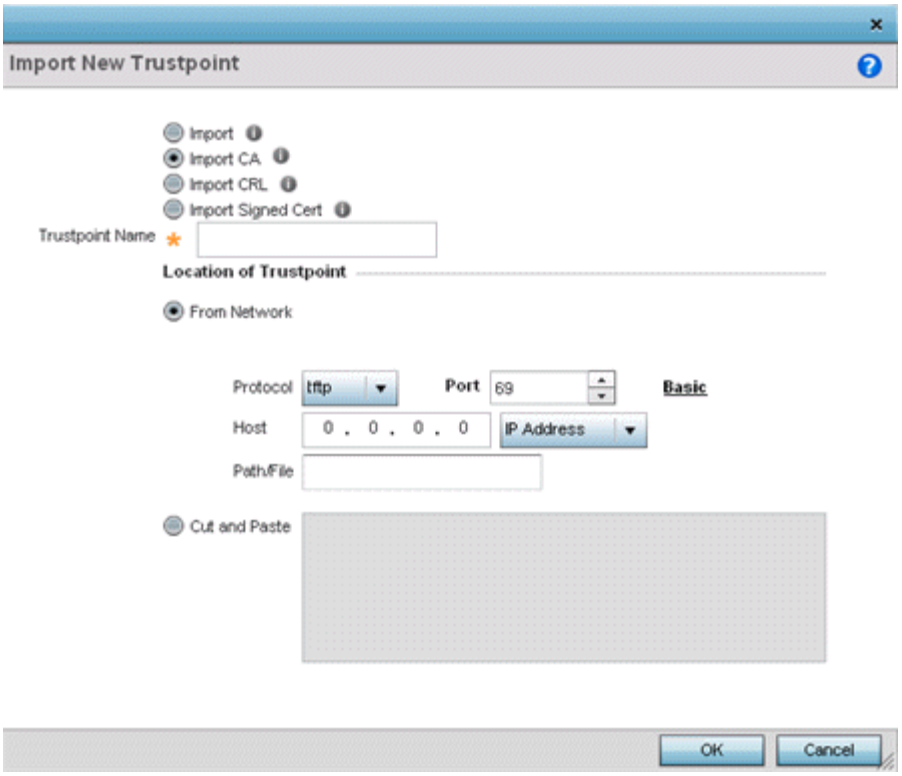



**Figure 422: Import New Trustpoint Screen**

1 To optionally import a CA certificate, select the **Import CA** button on the Import New Trustpoint screen.

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.




2 Define the following configuration parameters required to import a CA certificate:

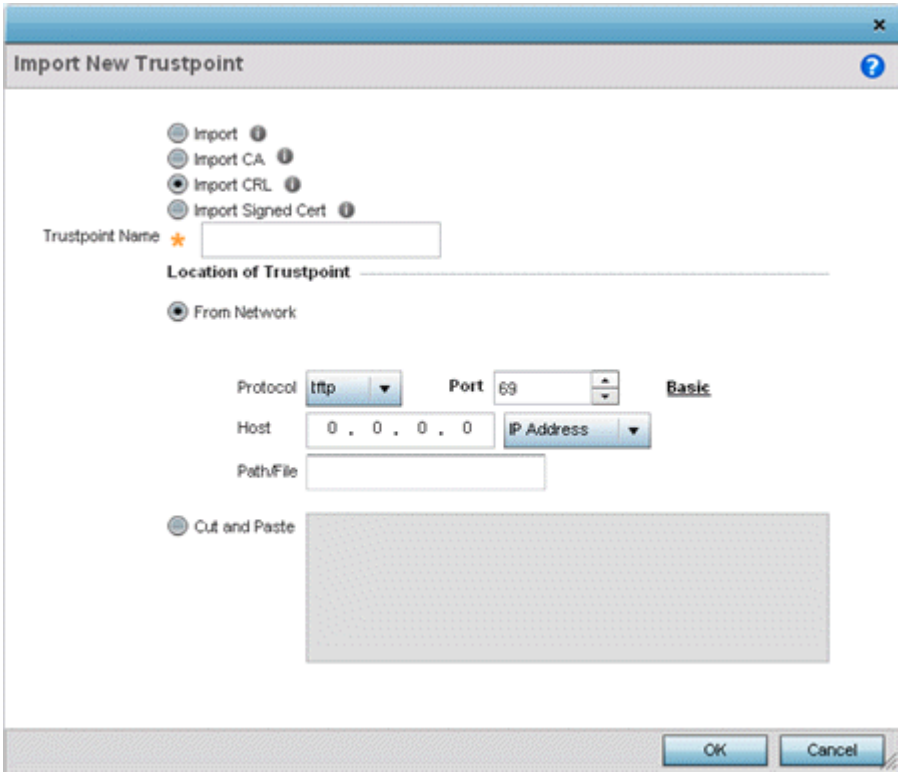
| | |
|---|---|
| Trustpoint Name | Enter the 32-character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, a corporation, or an individual. |
| URL | Provide the complete URL to the location of the trustpoint. If needed, click **Advanced** to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields that populate the screen is also dependent on the selected protocol. |
| Protocol | Select the protocol used for importing the target trustpoint. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1-4 |
| Port | Set the port. This option is not valid for **`cf`** and **`usb1-4`**. |

| | |
|---|---|
| Host | Provide the hostname string or numeric IP address of the server used to import the trustpoint. Hostnames cannot include an underscore character. This option is not valid for **`cf`** and **`usb1-4`**.<br>Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an IPv6 formatted address as the host. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Path/File | Specify the path to the trustpoint file. Enter the complete relative path to the file on the server. |

3 Select **OK** to import the defined CA certificate. Click **Cancel** to revert the screen to its last saved configuration.

4 To optionally import a CA certificate, select **Import CRL** button on the Certificate Management screen.

If a certificate displays in the Certificate Management screen with a CRL, that CRL can be imported. A CRL *(certificate revocation list)* is a list of certificates that have been revoked or are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.




5 Define the following configuration parameters required to import a CRL:

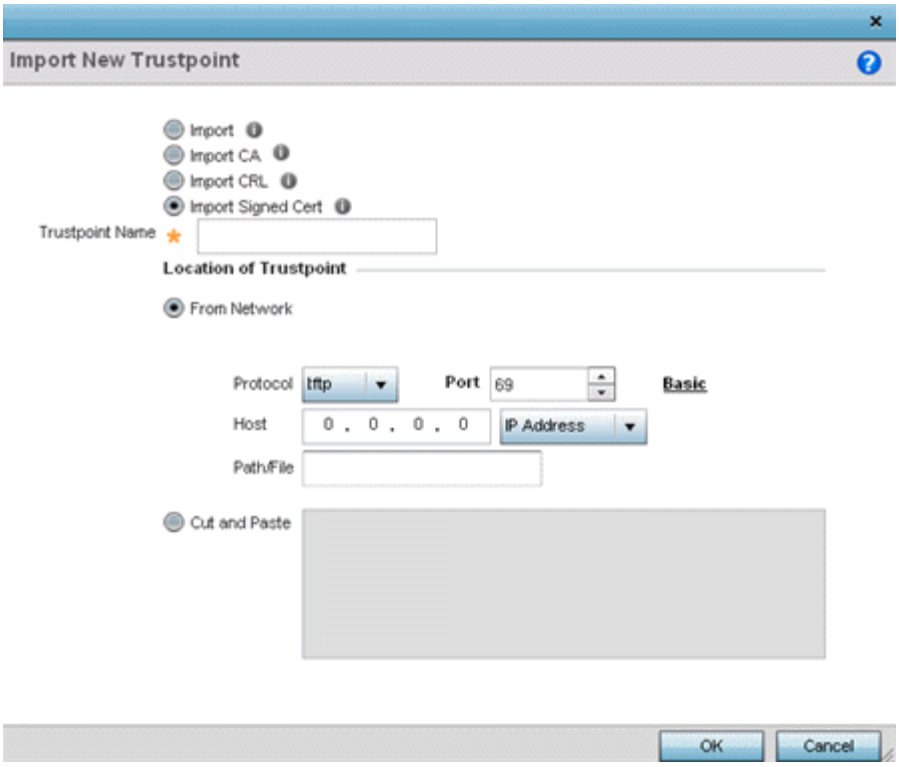
| | |
|---|---|
| Trustpoint Name | Enter the 32-character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate. |
| From Network | Select **From Network** to provide network address information to the location of the target CRL. The number of additional fields that populate the screen is also dependent on the selected protocol. This is the default setting. |
| URL | Provide the complete URL to the location of the CRL. If needed, click **Advanced** to expand the dialog to display network address information to the location of the CRL. The number of additional fields populating the screen depends on the selected protocol. |
| Advanced/Basic | Click **Advanced** or **Basic** to switch between a basic URL and an advanced location to specify trustpoint location. |
| Protocol | Select the protocol used for importing the CRL. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1-4 |
| Port | Set the port. This option is not valid for **`cf`** and **`usb1-4`**. |
| Host | Provide the hostname string or numeric IP address of the server used to import the CRL. Hostnames cannot include an underscore character. This option is not valid for **`cf`** and **`usb1-4`**.<br>Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an IPv6 formatted address as the host. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Path/File | Specify the path to the CRL file. Enter the complete relative path to the file on the server. |
| Cut and Paste | Select **Cut and Paste** to copy an existing CRL into the field. When pasting, no additional network address information is required. |

6 Select **OK** to import the CRL. Select **Cancel** to revert the screen to its last saved configuration.

7 To import a signed certificate, select the **Import Signed Cert** button on the Import New Trustpoint screen.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

Self-signed certificates cannot be revoked which may allow an attacker who has already gained controller access to monitor and inject data into a connection to spoof an identity if a private key has been compromised. However, CAs have the ability to revoke a compromised certificate, preventing its further use.




8 Define the following parameters required to Import a Signed Certificate:

| | |
|---|---|
| Certificate Name | Enter the 32-character maximum trustpoint name with which the certificate should be associated. |
| From Network | Select **From Network** to provide network address information to the location of the signed certificate. The number of additional fields that populate the screen is also dependent on the selected protocol. **From Network** is the default setting. |
| URL | Provide the complete URL to the location of the signed certificate. If needed, click **Advanced** to expand the dialog to display network address information to the location of the signed certificate. The number of additional fields populating the screen depends on the selected protocol. |
| Protocol | Select the protocol used for importing the signed certificate. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1-4 |
| Port | Set the port. This option is not valid for **`cf`** and **`usb1-4`**. |

| | |
|---|---|
| Host | Provide the hostname string or numeric IP address of the server used to import the signed certificate. Hostnames cannot include an underscore character. This option is not valid for **`cf`** and **`usb1-4`**.<br>Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an IPv6 formatted address as the host. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Path/File | Specify the path to the signed certificate file. Enter the complete relative path to the file on the server. |
| Cut and Paste | Select **Cut and Paste** to copy an existing certificate into the field. When pasting, no additional network address information is required. |

9 Select **OK** to import the signed certificate. Select **Cancel** to revert the screen to its last saved configuration.

### *Export Trustpoints*

Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

The trustpoints utilized by a controller, service platform or access point can be exported to an external resource for archive.

To export trustpoints:

1 Select **Operations → Manage Certificates**.

2 To optionally export a trustpoint to a remote location, select **Export** from the Certificate Management screen.

Once a certificate has been generated on the local authentication server, export the self signed certificate. A digital CA certificate is different from a self signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an active directory group policy for automatic root certificate deployment.

3 Additionally export the key to a redundant RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

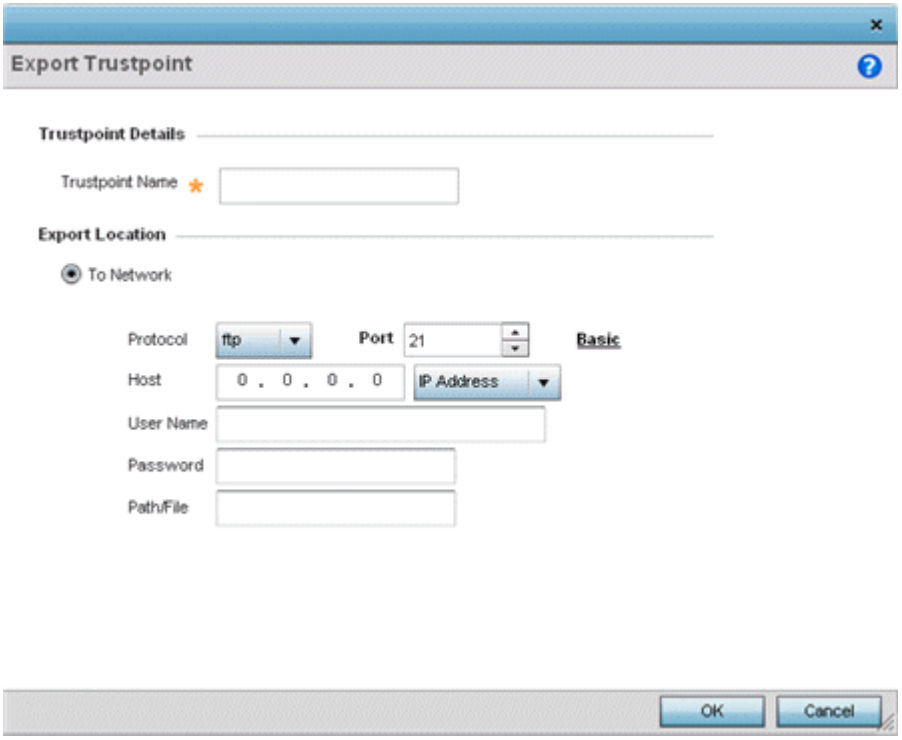



**Figure 423: Certificate Management - Export Trustpoint Screen**

4 Define the following configuration parameters required for the export of the trustpoint.

| | |
|---|---|
| Trustpoint Name | Enter the 32-character maximum name assigned to the trustpoint. The trustpoint signing the certificate can be a certificate authority, a corporation, or an individual.. |
| URL | Provide the complete URL to the location of the trustpoint. If needed, click **Advanced** to expand the dialog to display network address information to the location of the trustpoint. The number of additional fields populating the screen depends on the selected protocol. |
| Protocol | Select the protocol used for exporting the target trustpoint. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1-4 |
| Port | Set the port. This option is not valid for **cf** and **usb1-4**. |
| Host | Provide the hostname string or numeric IP address of the server used to export the trustpoint. Hostnames cannot include an underscore character. This option is not valid for **cf** and **usb1-4**.<br>Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an IPv6 formatted address as the host. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |

| | |
|---|---|
| Path/File | Specify the path to the signed trustpoint file. Enter the complete relative path to the file on the server. |
| Cut and Paste | Select **Cut and Paste** to copy an existing trustpoint into the field. When pasting, no additional network address information is required. |

5 Select **OK** to export the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

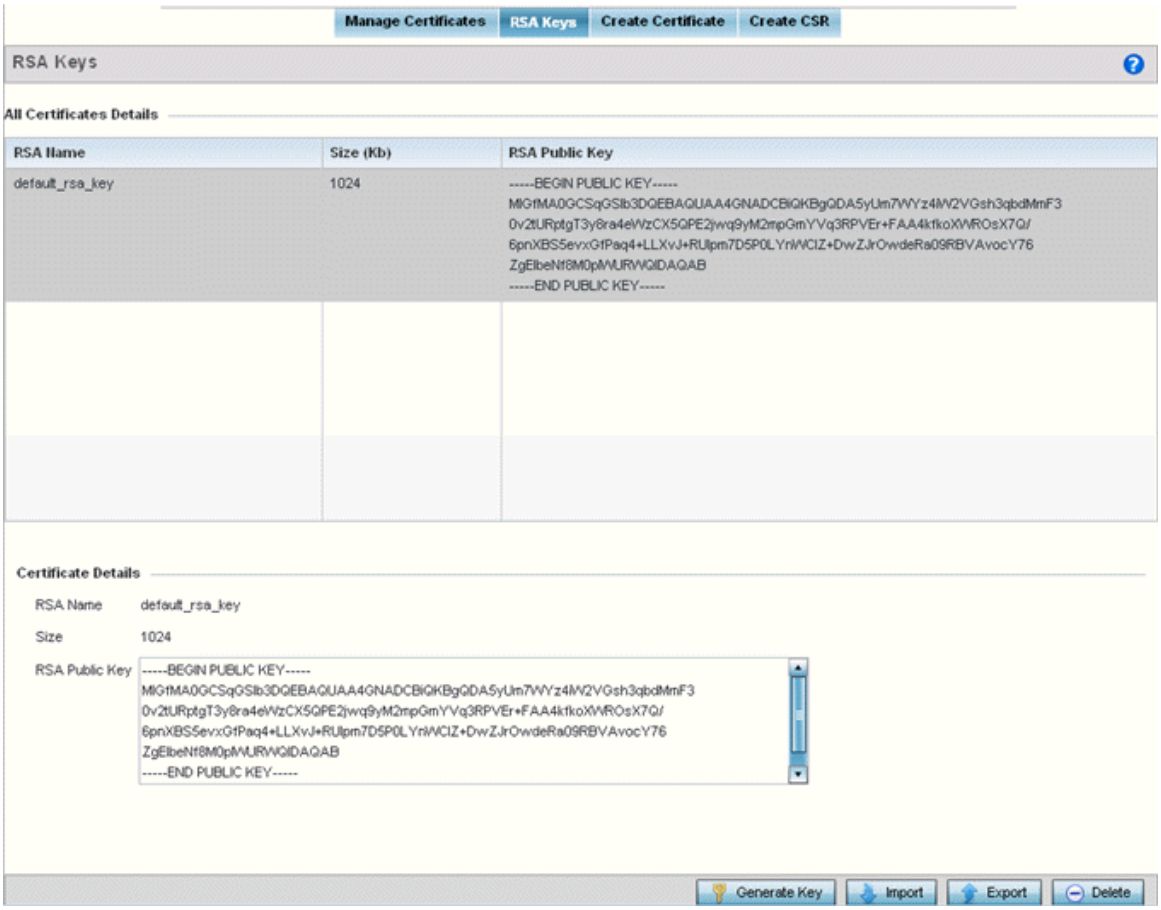
## RSA Key Management

Refer to the RSA Keys screen to review existing RSA key configurations applied to controller, service platform or access point managed devices. If an existing key does not meet the needs of a pending certificate request, generate a new key or import/export an existing key to and from a remote location.

*Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1 Select **RSA Keys** tab from the Certificate Management screen.




2 Select a listed device to review its current RSA key configuration.

Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key to a remote location or delete a key from a selected device.

3 Select **Generate Key** to create a new key with a defined size.

4 Define the following configuration parameters required for the Import of the key:

| | |
|---|---|
| Key Name | Enter the 32 character maximum name assigned to the RSA key. |
| Key Size | Use the spinner control to set the size of the key (from 1,024 - 2,048 bits). Consider leaving this value at the default setting to ensure optimum functionality. |

5 Select **OK** to generate the RSA key. Select **Cancel** to revert the screen to its last saved configuration.

*Import an RSA Key*

Controllers, service platforms and access point can import RSA keys utilized by other devices.

To Import an RSA Key:

1 Select **RSA Keys** tab from the Certificate Management screen.

2 To optionally import an RSA key, select **Import** from the **Certificate Management → RSA Keys** screen.

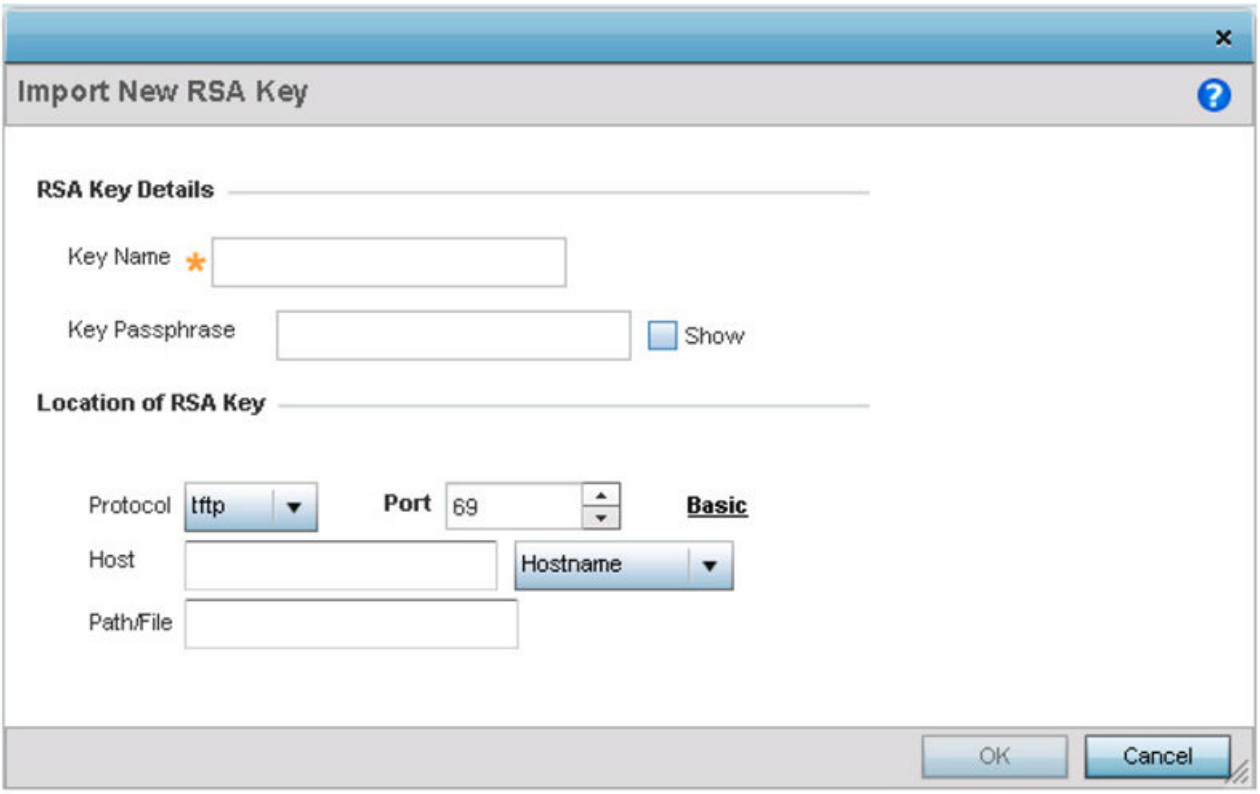



**Figure 424: Certificate Management - Import New RSA Key Screen**

3 Define the following parameters required for the Import of the RSA key:

| | |
|---|---|
| Key Name | Enter the 32-character maximum name assigned to identify the RSA key. |
| Key Passphrase | Define the key used by both the controller or service platform and the server (or repository) of the target RSA key. Click **Show** expose the actual characters used in the passphrase. When **Show** is not selected, the passphrase displays as a series of asterisks (****). |
| URL | Provide the complete URL to the location of the RSA key. If needed, click **Advanced** to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is dependent on the selected protocol. |
| Advanced/Basic | Select either **Advanced** or **Basic** to switch between a basic URL and an advanced location to specify key location. |
| Protocol | Select the protocol used for importing the target key. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1-4 |
| Port | Set the port. This option is not valid for **`cf`** and **`usb1-4`**. |
| Host | Provide the hostname string or numeric IP address of the server used to import the RSA key. Hostnames cannot include an underscore character. This option is not valid for **`cf`** and **`usb1-4`**.<br>Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an IPv6 formatted address as the host. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Path/File | Specify the path to the RSA key. Enter the complete relative path to the key on the server. |

4 Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

*Export an RSA Key*

The keys utilized by a controller, service platform or access point can be exported to an external resource for archive and future use.

Export the key to a redundant RADIUS server to import it without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

To export an RSA Key:

1 Select **Export** from the **Certificate Management → RSA Keys** screen.

The Export RSA Key window displays.

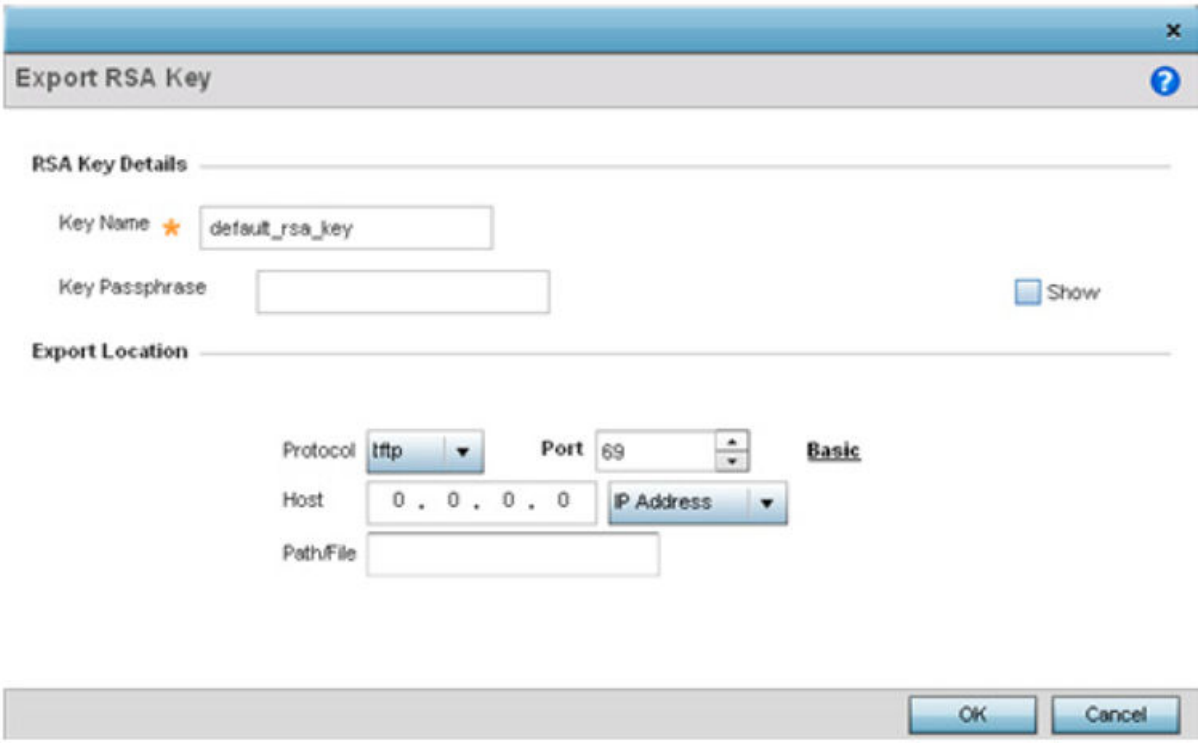



**Figure 425: Certificate Management - Export RSA Key Screen**

Export the key to a redundant RADIUS server to import it without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

2 Define the following configuration parameters required for the Export of the RSA key.

| | |
|---|---|
| Key Name | Enter the 32-character maximum name assigned to the RSA key. |
| Key Passphrase | Define the key used by both the controller or service platform and the server. Click **Show** expose the actual characters used in the passphrase. When **Show** is not selected, the passphrase displays as a series of asterisks (****). |
| URL | Provide the complete URL to the location of the key. If needed, click **Advanced** to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is dependent on the selected protocol. |
| Protocol | Select the protocol used for exporting the RSA key. Available options include:<br>• tftp<br>• ftp<br>• sftp<br>• http<br>• cf<br>• usb1-4 |
| Port | Set the port. This option is not valid for **`cf`** and **`usb1-4`**. |

| | |
|---|---|
| Host | Provide the hostname string or numeric IP address of the server used to export the RSA key. Hostnames cannot include an underscore character. This option is not valid for **`cf`** and **`usb1-4`**.<br>Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an IPv6 formatted address as the host. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Path/File | Specify the path to the key. Enter the complete relative path to the key on the server. |

3 Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

*Delete an RSA Key*

As keys become obsolete they can be deleted from their managing controller, service platform or access point.

To delete an RSA Key:

1 Select **RSA Keys** tab from the Certificate Management screen.
2 Select the **Delete** button from within the RSA Keys tab.
3 Provide the key name within the **Delete RSA Key** screen and select **Delete Certificates** to remove the certificate.
4 Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

## Certificate Creation

Use the Certificate Management screen to create new self-signed certificates. Self-signed certificates (often referred to as root certificates) do not use public or private CAs. A self-signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate that can be applied to a managed device:

1 In the Certificate Management screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.
2 Select **Create Certificate** from the upper, left-hand, side of the Certificate Management screen.

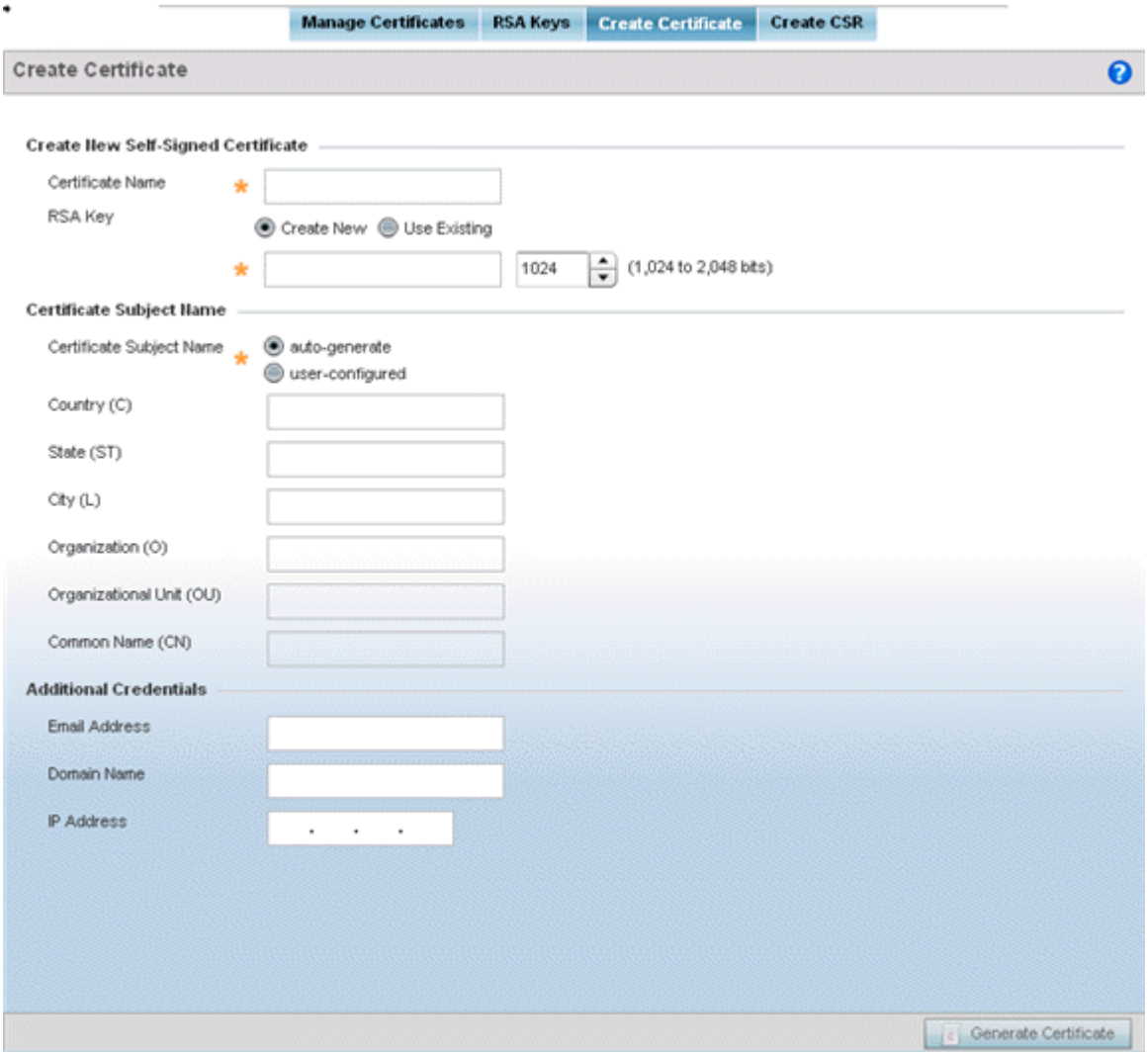



**Figure 426: Certificate Management - Create Certificate Screen**

3 Define the following configuration parameters required to **Create New Self-Signed Certificate**:

| | |
|---|---|
| Certificate Name | Enter the 32-character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate. |
| RSA Key | Select **Use Existing** and use the drop-down menu to set the key used by both the controller or service platform and the server (or repository) of the target RSA key Optionally, select **Create New** to enter a 32-character maximum name used to identify the RSA key. Set the size of the key to either 1,024 or 2,048 bits. We recommend leaving this value at the default setting of 2,048 to ensure optimum functionality. |

4 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

| | |
|---|---|
| Certificate Subject Name | Select either **auto-generate** to automatically create the certificate's subject credentials or **user-configured** to manually enter the credentials of the self-signed certificate. The default setting is **auto-generate**. |
| Country (C) | Define the country used in the certificate. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters. |
| State (ST) | Enter the state or province name used in the certificate. This is a required field. |
| City (L) | Enter a city to represent the city used in the certificate. This is a required field. |
| Organization (O) | Define the organization represented in the certificate. This is a required field. |
| Organizational Unit (OU) | Enter the organization unit represented in the certificate. This is a required field. |
| Common Name (CN) | If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here. |

5 Select the following **Additional Credentials** required for the generation of the self-signed certificate:

| | |
|---|---|
| Email Address | Provide an email address used as the contact address for issues relating to this certificate request. |
| Domain Name | Enter a *fully qualified domain name* (FQDN): an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added – for example, *somehost.example.com*. An FQDN differs from a regular domain name by its absoluteness, as a suffix is not added. |
| IP Address | Specify the IP address used as the destination for certificate requests. Only IPv4 formatted IP addresses are permitted. IPv6 formatted addresses are not permitted. |

6 Click **Generate Certificate** at the bottom of the Certificate Management > Create Certificate screen to produce the certificate.

## Generating a Certificate Signing Request

A CSR *(certificate signing request)* is a message from a requester to a certificate authority to apply for a digital certificate. The CSR is composed of a block of encrypted text generated on the server where the certificate will be used. It contains the organization name, common name (domain name), locality, and country.

An RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but it is used to digitally sign the completed request. The certificate created with a particular CSR only works with the private key generated with it. If the private key is lost, the certificate is no longer functional. The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1 In the Certificate Management screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.

2 Select **Create CSR** from the upper, left-hand, side of the Certificate Management screen.

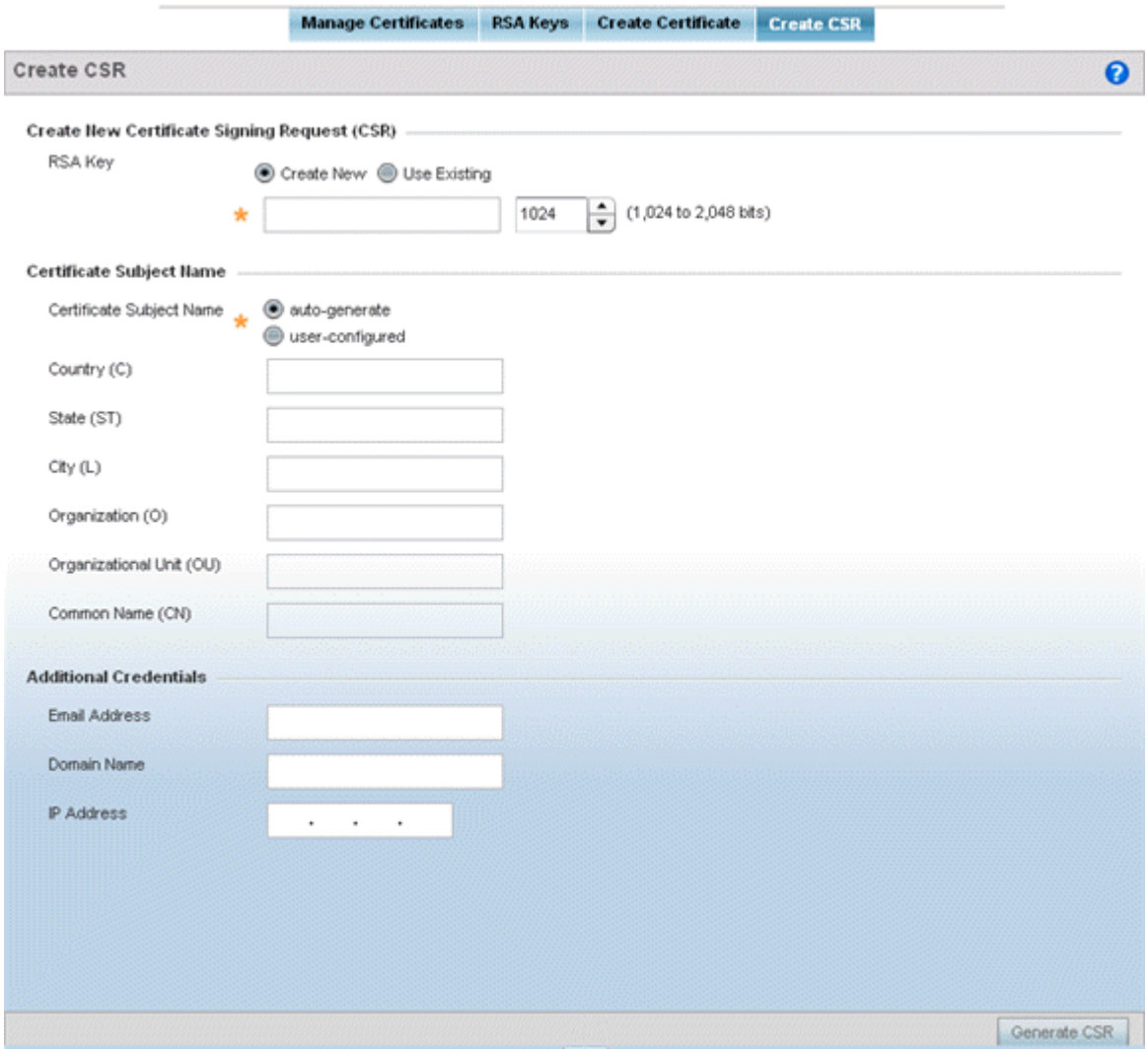



**Figure 427: Certificate Management - Create CSR Screen**

3 Define the following configuration parameter required to **Create New Certificate Signing Request (CSR)**:

| | |
|---|---|
| RSA Key | Select **Use Existing** and use the drop-down menu to set the key used by both the controller or service platform and the server (or repository) of the target RSA key Optionally, select **Create New** to enter a 32-character maximum name used to identify the RSA key. Set the size of the key to either 1,024 or 2,048 bits. We recommend leaving this value at the default setting of 2,048 to ensure optimum functionality. |

4 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

| | |
|---|---|
| Certificate Subject Name | Select either **`auto-generate`** to automatically create the certificate's subject credentials or **`user-configured`** to manually enter the credentials of the self-signed certificate. The default setting is **`auto-generate`**. |
| Country (C) | Define the country used in the CSR. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters. |

| | |
|---|---|
| State (ST) | Enter the state or province name represented in the CSR. This is a required field. |
| City (L) | Enter a city represented in the CSR. This is a required field. |
| Organization (O) | Define the organization represented in the CSR. This is a required field. |
| Organizational Unit (OU) | Enter the organization unit represented in the CSR. This is a required field. |
| Common Name (CN) | If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here. |

5 Select the following **Additional Credentials** required for the generation of the CSR:

| | |
|---|---|
| Email Address | Provide an email address used as the contact address for issues relating to this CSR. |
| Domain Name | Enter a *fully qualified domain name* (FQDN): an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added – for example, *somehost.example.com*. An FQDN differs from a regular domain name by its absoluteness, as a suffix is not added. |
| IP Address | Specify the IP address used as the destination for certificate requests. Only IPv4 formatted IP addresses are permitted. IPv6 formatted addresses are not permitted. |

6 Select **Generate CSR** to produce the CSR.

# Smart RF

*Self Monitoring At Run Time RF Management* (Smart RF) is an innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization and radio performance improvements.

The Smart RF functionality scans the managed network to determine the best channel and transmit power for each access point radio. Smart RF policies can be applied to specific RF Domains, to apply site specific deployment configurations and self recovery values to groups of devices within pre-defined physical RF coverage areas.

Smart RF also provides self recovery functions by monitoring the managed network in real-time and provides automatic mitigation from potentially problematic events such as radio interference, coverage holes and radio failures. Smart RF employs self recovery to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual reconfiguration to resolve.

Within the Operations node, Smart RF is managed within selected RF Domains, using the access points that comprise the RF Domain and their respective radio and channel configurations as the basis to conduct Smart RF calibration operations.

## Managing Smart RF for an RF Domain

When calibration is initiated, Smart RF instructs adopted radios (within a selected RF Domain) to beacon on a specific legal channel, using a specific transmit power setting. Smart RF measures the signal strength of each beacon received from both managed and unmanaged neighboring APs to define a RF map of the neighboring radio coverage area. Smart RF uses this information to calculate each managed radio's RF configuration as well as assign radio roles, channel and power.

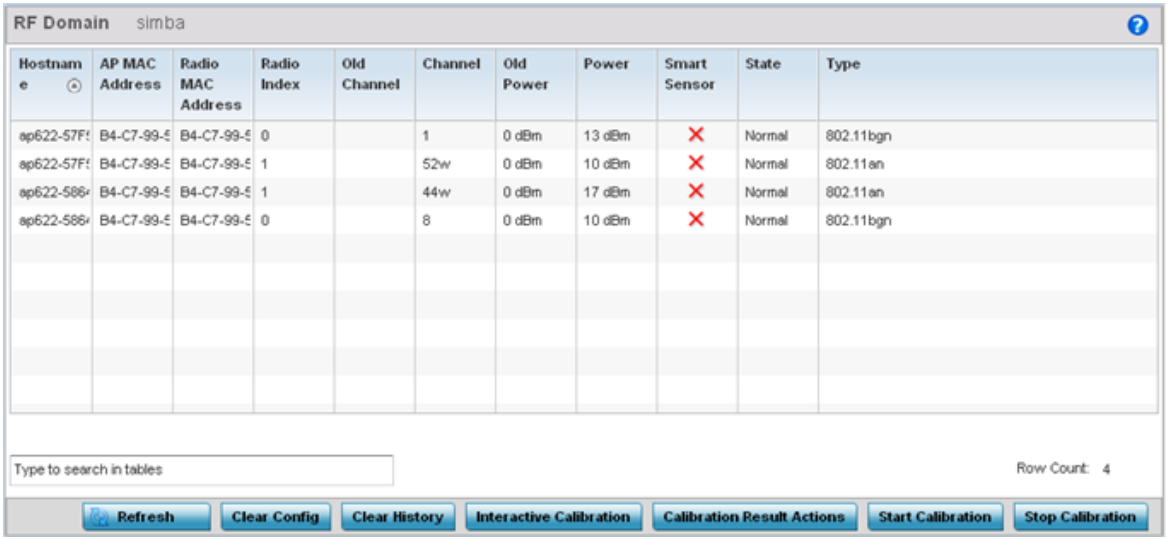
Within a well planned RF Domain, any associated radio should be reachable by at least one other radio. The Smart RF feature records signals received from its neighbors. access point to access point distance is recorded in terms of signal attenuation. The information is used during channel assignment to minimize interference.

To conduct Smart RF calibration for a controller, service platform or access point RF Domain:

1 Select **Operations**.

2 Select **Smart RF**.

3 The Smart RF screen displays information specific to the devices within the selected RF Domain using data from the last interactive calibration.




4 Refer to the following to determine whether a Smart RF calibration or an interactive calibration is required:

| | |
|---|---|
| Hostname | Displays the administrator assigned Hostname for each member of the RF Domain. |
| AP MAC Address | Displays the hardware encoded MAC address assigned to each access point radio within the selected RF Domain. This value cannot be modified as past of a calibration activity. |
| Radio MAC Address | Displays the hardware encoded MAC address assigned to each access point radio within the selected RF Domain. This value cannot be modified as part of a calibration activity. |
| Radio Index | Displays a numerical index assigned to each listed access point radio when it was added to the network. This index helps distinguish this radio from others within this RF Domain with similar configurations. This value is not subject to change as a result of a calibration activity, but each listed radio index can be used in Smart RF calibration. |
| Old Channel | Lists the channel originally assigned to each listed access point MAC address within this RF Domain. This value may have been changed as part an Interactive Calibration process applied to this RF Domain. Compare this Old Channel against the Channel value to right of it (in the table) to determine whether a new channel assignment was warranted to compensate for a coverage hole. |
| Channel | Lists the current channel assignment for each listed access point, as potentially updated by an Interactive Calibration. Use this data to determine whether a channel assignment was modified as part of an Interactive Calibration. If a revision was made to the channel assignment, a coverage hole was detected on the channel as a result of a potentially failed or under performing access point radio within this RF Domain. |

| | |
|---|---|
| Old Power | Lists the transmit power assigned to each listed access point MAC address within this RF Domain. The power level may have been increased or decreased as part an Interactive Calibration process applied to this RF Domain. Compare this Old Power level against the Power value to right of it (in the table) to determine whether a new power level was warranted to compensate for a coverage hole. |
| Power | This column displays the transmit power level for the listed access point MAC address after an Interactive Calibration resulted in a power adjustment. This is the new power level defined by Smart RF to compensate for a coverage hole. |
| Smart Sensor | Defines whether a listed access point is smart sensor on behalf of the other access point radios comprising the RF Domain. |
| State | Displays the current state of the Smart RF managed access point radio. Possible states include: *Normal*, *Offline* and *Sensor*. |
| Type | Displays the radio type (802.11an, 802.11bgn etc.) of each listed access point radio within the selected RF Domain. |

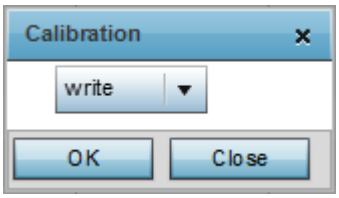
5 Select the **Refresh** button to (as needed) to update the contents of the Smart RF screen and the attributes of the devices within the selected RF Domain.

Note

Smart RF is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections.

6 Select the **Interactive Calibration** button to initiate a Smart RF calibration using the access points within the selected RF Domain. The results of the calibration display within the Smart RF screen. Of particular interest are the channel and power adjustments made by the controller's Smart RF module. Expand the screen to display the Event Monitor to track the progress of the Interactive Calibration.

7 Select the **Calibration Result Actions** button to launch a sub screen used to determine the actions taken based on the results of the Interactive Calibration. The results of an Interactive calibration are not applied to radios directly, the administrator has the choice to select one of following options:




| | |
|---|---|
| Replace | Overwrites the current channel and power values with new channel power values the Interactive Calibration has calculated. |
| Write | Writes the new channel and power values to the radios under their respective device configurations. |
| Discard | Discards the results of the Interactive Calibration without applying them to their respective devices. |

8 Select the **Run Calibration** option to initiate a calibration. New channel and power values are applied to radios, they are not written to the running-configuration.

These values are dynamic and may keep changing during the course of the run-time monitoring and calibration the Smart RF module keeps performing to continually maintain good coverage. Unlike an Interactive Calibration, the Smart RF screen is not populated with the changes needed on access

point radios to remedy a detected coverage hole. Expand the screen to display the Event Monitor to track the progress of the calibration.

9 The calibration process can be stopped by selecting the **Stop Calibration** button.

## Operations Deployment Considerations

Before defining the access point's configuration using the Operations menu, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- If an access point's (or its associated device's) firmware is older than the version on the support site, update to the latest firmware version for full functionality and utilization.
- An access point must be rebooted to implement a firmware upgrade. Take advantage of the reboot scheduling mechanisms available to the access point to ensure its continuously available during anticipated periods of heavy wireless traffic utilization.
- In a well planned RF Domain, any associated radio should be reachable by at least one other radio. Keep this in mind when utilizing the Smart RF feature to record signals from neighboring access points. Access point to access point distance is recorded in terms of signal attenuation.

# 14 Statistics



This chapter describes statistics displayed by the GUI *(graphical user interface)*. Statistics are available for access point and their managed devices.

A Smart RF statistical history is available to assess adjustments made to device configurations to compensate for detected coverage holes or device failures.

Statistics display detailed information about peers, health, device inventories, wireless clients associations, adopted AP information, rogue APs and WLANs. Access point statistics can be exclusively displayed to validate connected access points, their VLAN assignments and their current authentication and encryption schemes.

Wireless client statistics are available for an overview of client health. Wireless client statistics includes RF quality, traffic utilization and user details. Use this information to assess if configuration changes are required to improve network performance.

System wide statistics are available to review the health of the entire wireless network, including all its RF Domains and member devices.

RF Domain statistics are available to administrate specific device groups (domains) created in respect to their shared deployment objective.

Access Point statistics can be exclusively displayed to validate connected access points, their VLAN assignments and their current authentication and encryption schemes.

Wireless Client statistics are available for an overview of client health. Wireless client statistics includes RF quality, traffic utilization and user details. Use this information to assess if configuration changes are required to improve network performance.

Guest Access statistics are also available for the periodic review of wireless clients requesting the required pass code, authentication and access into the WiNG managed guest network.

For more information, see:

- System Statistics on page 913
- RF Domain Statistics on page 922
- Access Point Statistics on page 973
- Wireless Client Statistics on page 1093

# System Statistics

The System screen displays information supporting managed devices (wireless controllers, service platforms, access points and their connected wireless clients). Use this information to asses the overall state of the devices comprising the system. Systems data is organized as follows:

The data is organized as follows:

- Health
- Inventory
- Adopted Devices
- Pending Adoptions
- Offline Devices
- Device Upgrade
- WIPS Summary

The following devices can report system data:

- Access Points - AP 6522, AP 6562, AP 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP-7612, AP 7622, AP7632, AP7662, AP-8163, AP-8432, AP-8533
- Wireless Controllers - RFS 4000
- Service Platforms - NX 5500, NX 7510, NX 95XX, NX 96XX, VX

## Health

The Health screen displays the overall performance of the managed network (system). This includes device availability, overall RF quality, resource utilization and network threat perception.

To display the health of the managed network:

1 Select the **Statistics** → **System** menu from the Web UI.
2 Select **Health** from the left-hand side of the UI.

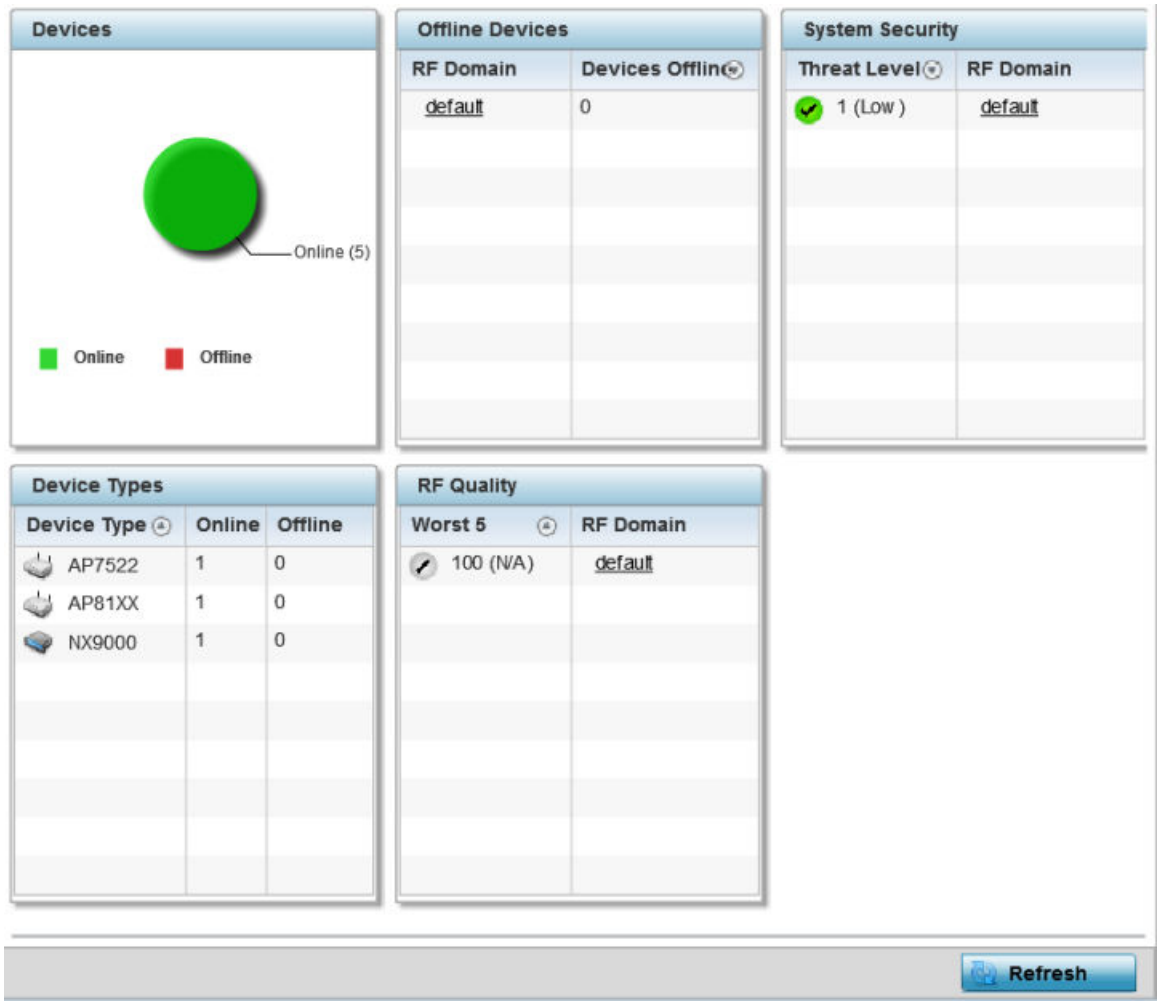



**Figure 428: Statistics - System - Health Screen**

3 The Devices table displays the total number of devices in the access pointmanaged network. The pie chart is a proportional view of how many devices are functional and currently online. Green indicates online devices and red offline devices detected within the managed network.

4 The Offline Devices table displays a list of devices in the controller managed network that are currently offline.

The table displays the number of offline devices within each impacted RF Domain. Assess whether the configuration of a particular RF Domain is contributing to an excessive number of offline devices.

5 The Device Types table displays the kinds of devices detected within the system. Each device type displays the number currently online and offline.

6 Use the RF Quality table to isolate poorly performing radio devices within specific controller managed RF Domains. This information is a starting point to improving the overall quality of the wireless controller managed network. The RF Quality area displays the RF Domain performance.

Refer to the following table for details:

| | |
|---|---|
| Worst 5 | Displays five RF Domains with the lowest quality indices in the wireless controller managed network. The value can be interpreted as:<br>• 0-50 – Poor Quality<br>• 50-75 – Medium Quality<br>• 75-100 – Good Quality |
| RF Domain | Displays the name of the RF Domain wherein system statistics are polled for the poorly performing device. |

7 The System Security table defines a Threat Level as an integer value indicating a potential threat to the system. It is an average of the threat indices of all the RF Domains managed by the access point.

| | |
|---|---|
| Threat Level | Displays the threat perception value. This value can be interpreted as:<br>• 0-2 – Low threat level<br>• 3-4 – Moderate threat level<br>• 5 – High threat level |
| RF Domain | Displays the name of the target RF Domain for which the threat level is displayed. |

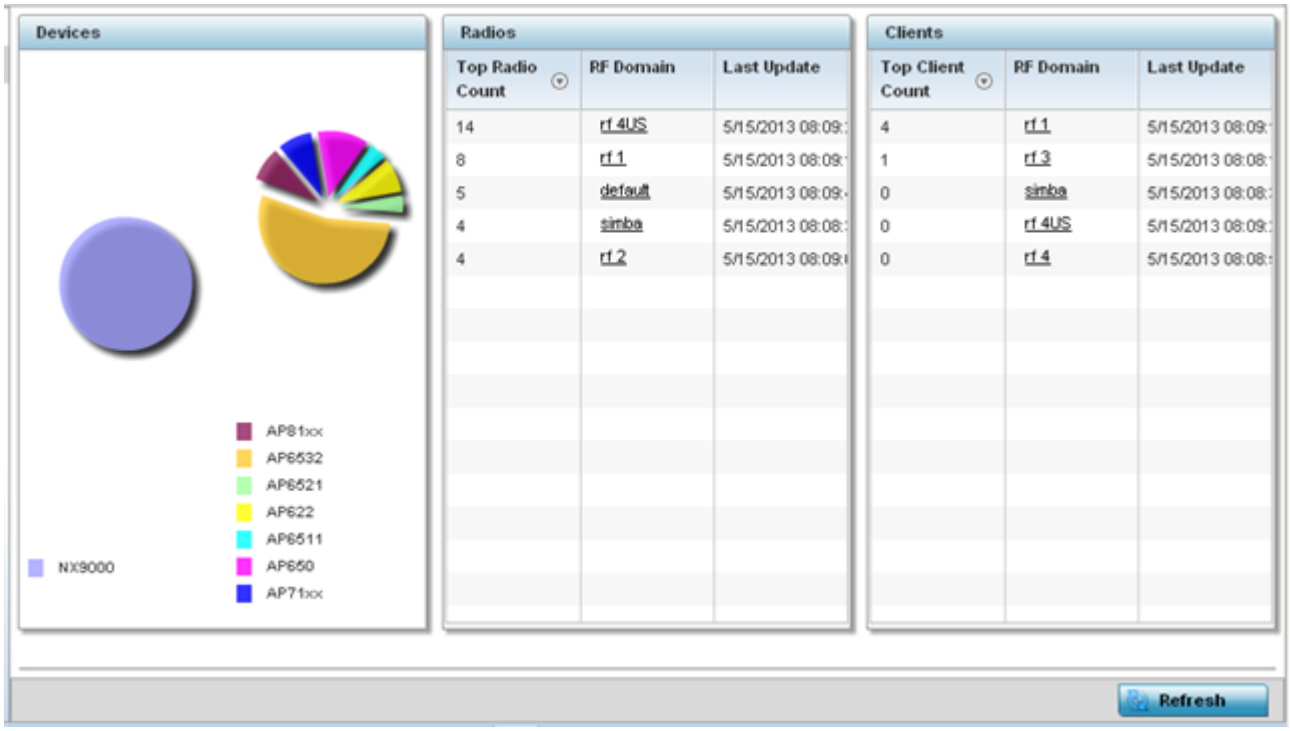
8 Select **Refresh** at any time to update the statistics counters to their latest values.

## Inventory

The Inventory screen displays information about the physical hardware managed within the system by its member controller or service platforms. Use this information to assess the overall performance of wireless devices.

To display the inventory statistics:

1 Select Inventory from the left-hand side of the UI.




2 The **Devices** table displays an exploded pie chart depicting the controller, service platform and access point device type distribution by model. Use this information to assess whether these are the correct models for the system's deployment objective.

3 The **Radios** table displays radios deployed within the access point managed network. This area displays the total number of managed radios and the top 5 RF Domains in terms of radio count. The **Total Radios** value is the total number of radios in this system.

| | |
|---|---|
| Top Radio | Displays the radio index for each listed top performing radio. |
| RF Domain | Displays the name of the RF Domain where the listed radios reside as device members. The RF Domain displays as a link that can be selected to display specific RF Domain member radio configuration information in greater detail. |
| Last Update | Displays the UTC time stamp when each listed radio was last reported. |

4 The **Clients** table displays the total number of wireless clients managed by the access point. This Top Client Count table lists the top 5 RF Domains, in terms of the number of wireless clients adopted:

| | |
|---|---|
| Top Client | Displays the client index of each listed top performing client. |
| RF Domain | Displays the name of the client RF Domain. |
| Last Update | Displays the UTC timestamps when the client count was last reported. |

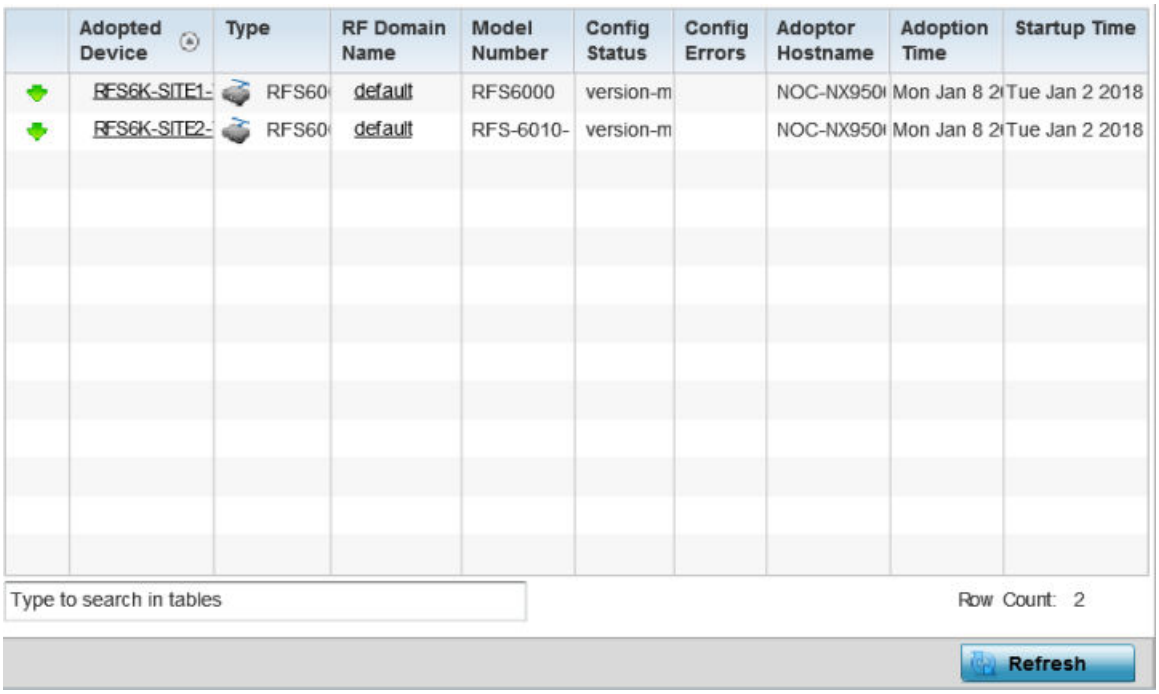
5 Select **Refresh** to update the statistics counters to their latest values.

## Adopted Devices

The **Adopted Devices** screen displays a list of devices adopted to the access point managed network. Use this screen to view a list of devices and their current status.

To view adopted device statistics:

1 Select the **Statistics** menu from the Web UI.
2 Select the **System** node from the left navigation pane.
3 Select **Adopted Devices** from the left-hand side of the UI.




The **Adopted Devices** screen displays the following information:

| | |
|---|---|
| Adopted Device | Displays the administrator assigned hostname of the adopted device. Select the adopted device link to display configuration and network address information in greater detail. |
| Type | Displays the adopted access point's model type. |
| RF Domain Name | Displays the domain the adopted AP has been assigned. Select the RF Domain link to display configuration and network address information in greater detail for member devices. |
| Model Number | Lists the model number of each AP that has been adopted since this screen was last refreshed. |
| Config Status | Displays the configuration file version in use by each listed adopted device. Use this information to determine whether an upgrade would increase the functionality of the adopted device. |
| Config Errors | Lists any errors encountered when the listed device was adopted. |
| Adopter Hostname | Lists the administrator hostname assigned to the adopting controller, service platform or access point. |
| Adoption Time | Displays a timestamp for each listed device reflecting when the device was adopted. |
| Startup Time | Provides a date stamp when the adopted device was restarted post adoption |

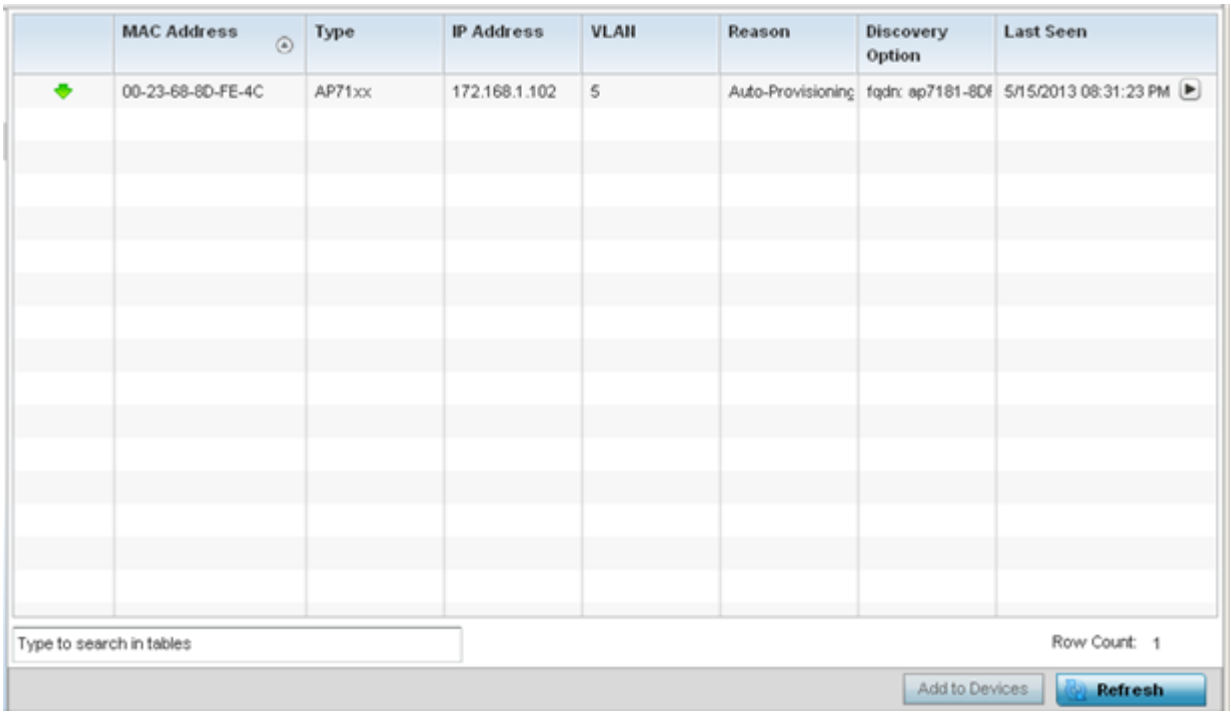
4 Click **Refresh** to update the statistics counters to their latest values.

## Pending Adoptions

The **Pending Devices** screen displays those devices detected within an access point managed coverage area, but have yet to be adopted. Review these devices to assess whether they are good available resources to provide services to requesting clients and peer radio devices.

To view pending adoptions:

1 Select the **Statistics** menu from the Web UI.
2 Select the **System** node from the left navigation pane.
3 Select **Pending Adoptions** from the left-hand side of the UI.




The **Pending Adoptions** screen displays the following information:

| | |
|---|---|
| MAC Address | Displays the MAC address of the device pending adoption. Select the MAC address to view device configuration and network address information in greater detail. |
| Type | Displays the device's model type. |
| IP Address | Displays the current IP address of the device pending adoption. |
| VLAN | Displays the VLAN the pending device uses as a virtual interface once adopted. |
| Reason | Displays a status (reason) as to why the device is pending adoption. |
| Discovery Option | Displays the discovery option code for each AP listed pending adoption. |
| Last Seen | Displays the date and time stamp of the last time the device was seen. Click the arrow next to the date and time to toggle between standard time and UTC. |
| Add to Devices | Select a listed AP and select the **Add to Devices** button to begin the adoption process for this detected AP. |

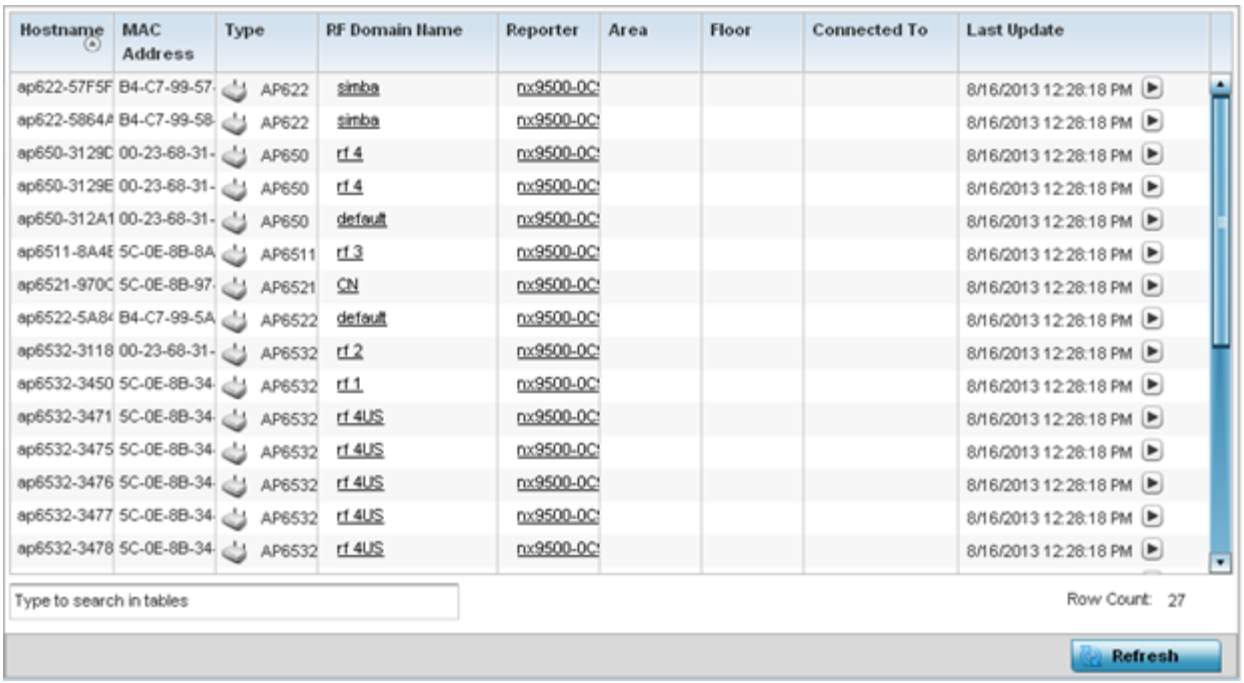
4 Click **Refresh** to update the statistics counters to their latest values.

## Offline Devices

The **Offline Devices** screen displays a list of devices within the managed network or RF Domain that are currently off line. Review the contents of this screen to help determine whether an offline devices requires administration.

To view offline devices potentially available for adoption:

1 Select the **Statistics** menu from the Web UI.
2 Select the **System** node from the left navigation pane.
3 Select **Offline Devices** from the left-hand side of the UI.




The **Offline Devices** screen lists the following information:

| | |
|---|---|
| Hostname | Lists the administrator assigned hostname provided when the device was added to the network. |
| MAC Address | Displays the factory encoded MAC address of each listed offline device. |
| Type | Displays the AP model type. |
| RF Domain Name | Displays the name of the offline device's RF Domain membership, if applicable. Select the RF Domain link to display configuration and network address information in greater detail. |
| Reporter | Displays the administrator assigned hostname of the device reporting a device as offline. Select the reporting device link to display configuration and network address information in greater detail. |
| Area | Lists the administrator assigned deployment area where the offline device is detected. |
| Floor | Lists the administrator assigned deployment floor where the offline device is detected. |

| | |
|---|---|
| Connected To | Lists the offline device's connected controller, service platform or peer model access point. |
| Last Update | Displays a date and time stamp for the last time the listed device was detected within the managed network.<br>Select the arrow next to the date and time to toggle between standard time and UTC. |

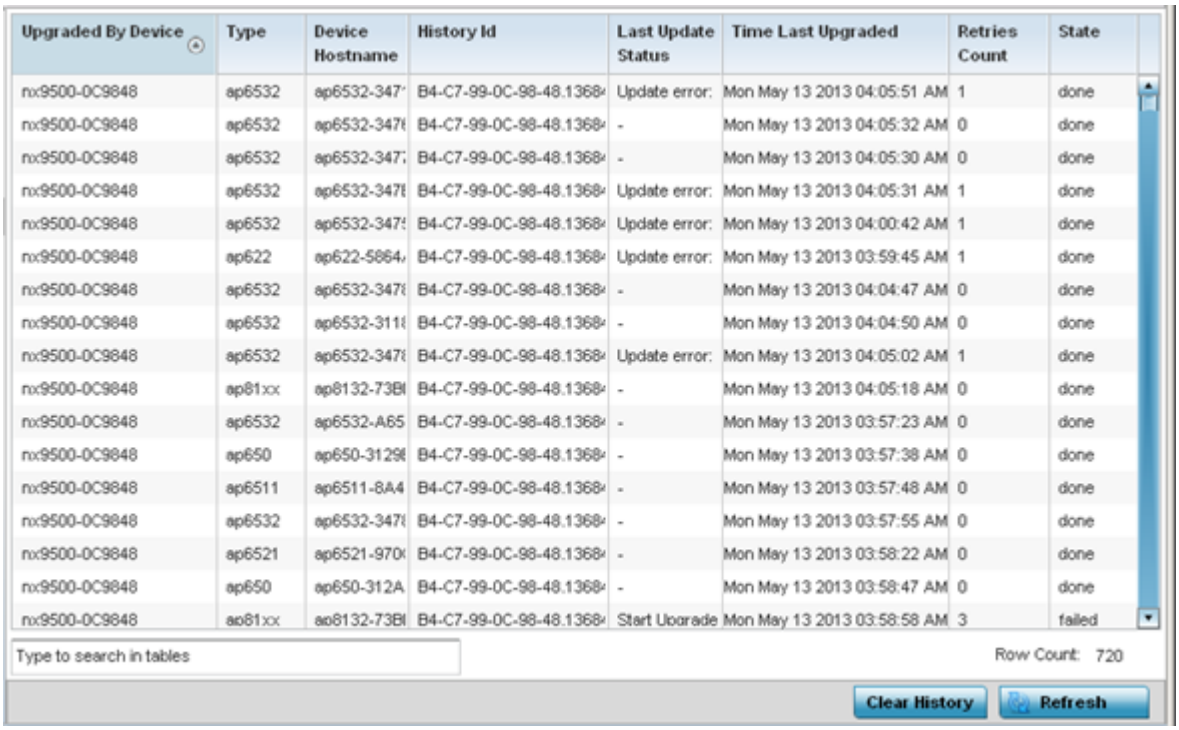
4 Click **Refresh** to update the statistics counters to their latest values.

## Device Upgrade

The Device Upgrade screen displays available licenses for devices within a cluster. It displays the total number of AP licenses.

To view upgrade statistics at a system level:

1 Select the Statistics menu from the Web UI.
2 Select the System node from the left navigation pane.
3 Select Device Upgrade from the left-hand side of the UI.




The Device Upgrade screen displays the following information:

| | |
|---|---|
| Upgraded By Device | Displays the MAC address of the controller, service platform or peer model access point that performed an upgrade. |
| Type | Displays the model of the access point. |
| Device Hostname | Displays the administrator-assigned hostname of the access point or the device receiving the update. |
| History ID | Displays a unique timestamp for the upgrade event. |
| Last Update Status | Displays the initiation, completion or error status of each listed upgrade operation. |

| | |
|---|---|
| Time Last Upgraded | Displays the date and time of the last upgrade operation. |
| Retries Count | Displays the number of retries made in an update operation. |
| State | Displays the **done** or **failed** state of an upgrade operation. |

4 Click **Clear History** to clear the screen of its current status and begin a new data collection.

5 Click **Refresh** to update the statistics counters to their latest values.

## WIPS Summary

The WIPS *(Wireless Intrusion Protection System)* provides continuous protection against wireless threats and acts as an additional layer of security complementing wireless VPNs and existing encryption and authentication policies. Controllers and service platforms support WIPS through the use of dedicated sensor devices, designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block devices using manual termination, air lock down or port suppression.

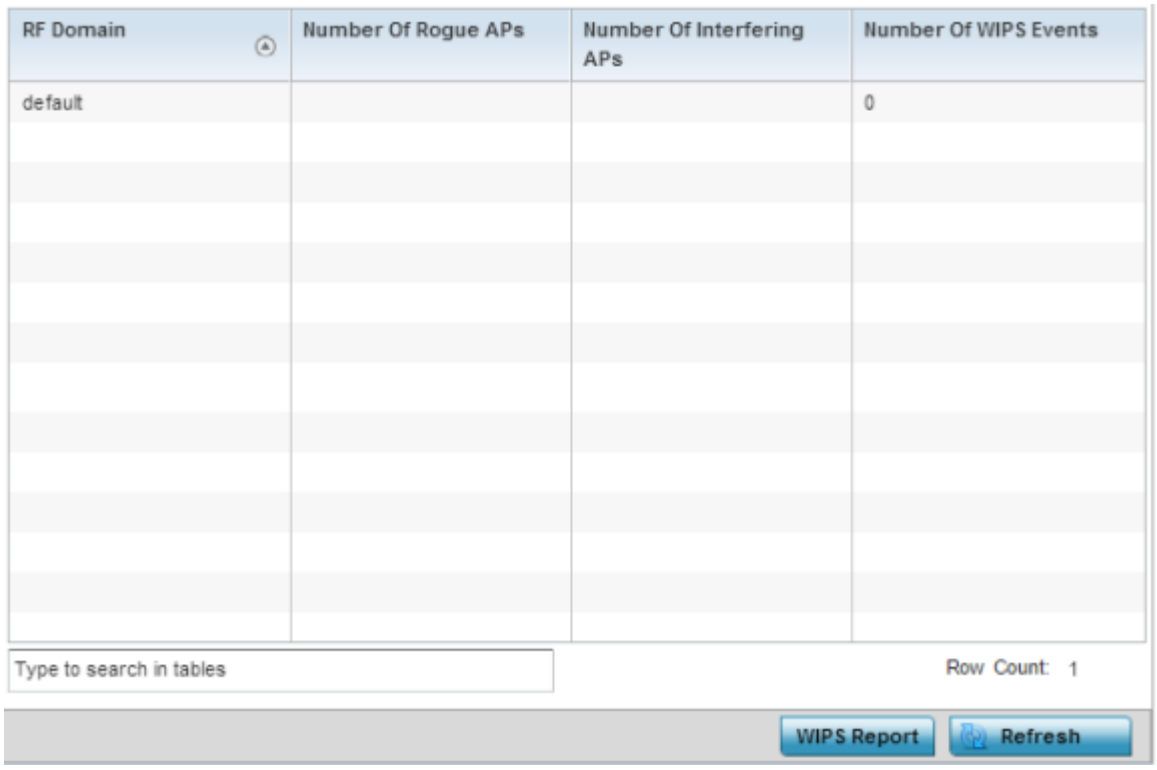
The WIPS Summary screen lists RF Domains residing in the system and reports the number of unauthorized and interfering devices contributing to the potential poor performance of the RF Domain's network traffic. Additionally, the number of WIPS events reported by each RF Domain is also listed to help an administrator better mitigate risks to the network.

To review and assess the impact of rogue and interfering APs, as well as the occurrence of WIPS events within the managed system:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **WIPS Summary** from the left-hand side of the UI.



4 Refer to the following WIPS data reported for each RF Domain in the system:

| | |
|---|---|
| RF Domain | Lists the RF Domain within the system reporting rogue and interfering AP event counts. Use this information to assess whether a particular RF Domain is reporting an excessive number of events or a large number of potentially invasive rogue APs versus the other RF Domains within the controller, service platform or AP managed system. |
| Number of Rogue APs | Displays the number of unsanctioned devices in each listed RF Domain. Unsanctioned devices are those devices detected within the listed RF Domain, but have not been deployed by a administrator as a known and approved controller, service platform or AP managed device. |
| Number of Interfering APs | Displays the number of devices exceeding the interference threshold in each listed RF Domain. Each RF Domain utilizes a WIPS policy with a set interference threshold (from -100 to -10 dBm). When a device exceeds this *noise* value, it is defined as an interfering access point capable of disrupting the signal quality of other sanctioned devices operating below an approved RSSI maximum value. |
| Number of WIPS Events | Lists the number of devices triggering a WIPS event within each listed RF Domain. Each RF Domain utilizes a WIPS policy where excessive, MU and AP events can have their individual values set for event generation. An administrator can **`enable`** or **`disable`** the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action. |

5 Select the **WIPS Report** button to launch a sub-screen to filter how WIPS reports are generated for the system.


6 Select one of the following options to refine event reporting to a specific type of WIPS activity.
- **Only Rogue APs**
- **Only Interferer APs**
- **All APs**

7 Click **Generate Report** to compile and archive the results of the query.

8 Click **Refresh** to update the screen's statistics counters to their latest values.

## RF Domain Statistics

The RF Domain screens display status for a selected controller, service platform or access point RF Domain. This includes the RF Domain *health* and *device inventory, wireless clients* and *Smart RF* functionalities. RF Domains allow administrators to assign regional, regulatory and RF configuration to devices deployed in a common coverage area, such as on a building floor or site. Each RF Domain contains regional, regulatory and sensor server configuration parameters and may also be assigned policies that determine Access, SMART RF and WIPS configuration.

Unlike controllers and service platforms, access point RF Domains are comprised of just other APs.

Use the following information to obtain an overall view of the performance of the selected RF Domain and troubleshoot issues with the domain or any member device.

- Health
- Inventory
- Devices
- AP Detection
- Device Upgrade
- Wireless Clients
- Wireless LANs
- Radios
- Bluetooth
- Mesh
- Mesh Point
- SMART RF
- WIPS
- Captive Portal
- Coverage Hole Detection

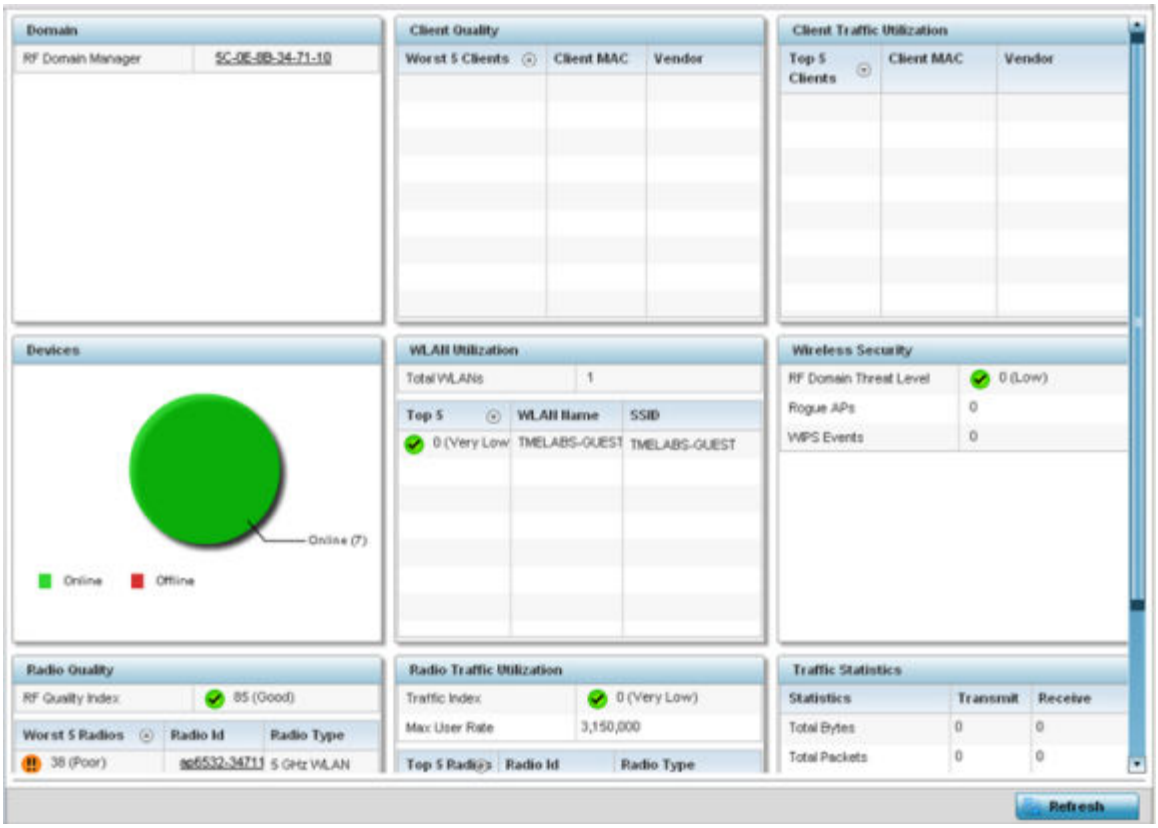
## Health

The **Health** screen displays general status information for a selected RF Domain, including data polled from all its members.

To display the collective device membership health of a controller, service platform or AP RF Domain:

1 Select the **Statistics** → **System** menu from the Web UI.
2 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.




3 Review the different fields displayed on the **RF Domain > Health** screen:

- Domain - Displays the name of the RF Domain manager. The RF Domain manager is the focal point for the radio system and acts as a central registry of applications, hardware and capabilities. It also serves as a mount point for all the different pieces of the hardware system file.
- Devices - Displays the total number of online versus offline devices in the RF Domain, and an exploded pie chart depicts their status.
- Radio Quality - Displays information on the RF Domain's RF quality. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions, as well as the retry and error rate. This area also lists the worst 5 performing radios amongst all the RF Domain device member radios.

  The RF Quality Index can be interpreted as:

  - 0-20 – Very poor quality
  - 20-40 – Poor quality
  - 40-60 – Average quality
  - 60-100 – Good quality

  Refer to the Radio Quality table for RF Domain member radios requiring administration to improve performance:

| | |
|---|---|
| Worst 5 Radios | Displays five radios with the lowest average quality in the RF Domain. |
| Radio ID | Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 or radio 3). |
| Radio Type | Displays the radio type as either 5 GHz or 2.4 GHz. |

- Client Quality - Refer to the table below for RF Domain connected clients requiring administration to improve performance:

| | |
|---|---|
| Worst 5 Clients | Displays the five clients having the lowest average quality indices. |
| Client MAC | Displays the hard coded radio MAC of the wireless client. |
| Vendor | Displays the vendor name of the wireless client. |

- WLAN Utilization - Refer to the table below to assess WLAN related information:

| | |
|---|---|
| Total WLANs | Displays the total number of WLANs managed by RF Domain member access points. |
| Top 5 | Displays the five RF Domain utilized WLANs with the highest average quality indices. |
| WLAN Name | Displays the WLAN Name for each of the Top 5 WLANs in the access point RF Domain. |
| SSID | Displays the SSID for the WLAN. |

- Radio Traffic Utilization - Refer to the following table to identify radios requiring administration to improve performance:

| | |
|---|---|
| Max. User Rate | Displays the maximum recorded user rate in kbps. |
| Top 5 Radios | Displays five radios with the best average quality in the RF Domain. |
| Radio ID | Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 or radio 3). |
| Radio Type | Displays the radio type as either 5 GHz or 2.4 GHz. |

- Client Traffic Utilization - Refer to the following table for wireless client related information:

| | |
|---|---|
| Top 5 Clients | Displays the five clients having the highest average quality indices. |
| Client MAC | Displays the client's hard coded MAC address used a hardware identifier. |
| Vendor | Lists each client's manufacturer. |

- Wireless Security - Indicates the security of the transmission between WLANs and the wireless clients they support. This value indicates the vulnerability of the WLANs.

| | |
|---|---|
| RF Domain Threat Level | Indicates the threat from wireless clients trying to find network vulnerabilities within the RF Domain. The threat level is represented by an integer. |
| Rogue APs | Lists the number of unauthorized APs detected by RF Domain member devices. |
| WIPS Events | Lists the number of WIPS events generated by RF Domain member devices. |

- Traffic Statistics - Displays the following information for transmitted and received packets:

| | |
|---|---|
| Total Bytes | Displays the total bytes of data transmitted and received within the RF Domain. |
| Total Packets | Lists the total number of data packets transmitted and received within the RF Domain. |
| User Data Rate | Lists the average user data rate within the RF Domain. |

| | |
|---|---|
| Bcast/Mcast Packets | Displays the total number of broadcast/multicast packets transmitted and received within the RF Domain. |
| Management Packets | Displays the total number of management packets processed within the RF Domain. |
| Tx Dropped Packets | Displays the total number of dropped data packets within the RF Domain. |
| Rx Errors | Displays the number of errors encountered during data transmission within the RF Domain. The higher the error rate, the less reliable the connection or data transfer. |

- SMART RF Activity - Refer to the table below for details:

| | |
|---|---|
| Time Period | Lists the time period when Smart RF calibrations or adjustments were made to compensate for radio coverage holes or interference. |
| Power Changes | Displays the total number of radio transmit power changes that have been made using SMART RF within the RF Domain. |
| Channel Changes | Displays the total number of radio transmit channel changes that have been made using SMART RF within the RF Domain. |
| Coverage Changes | Displays the total number of radio coverage area changes that have been made using SMART RF within the RF Domain. |

4 Periodically click **Refresh** to update the contents of the screen to their latest values.

## Inventory

The Inventory screen displays an inventory of RF Domain member APs, connected wireless clients, wireless LAN utilization and radio availability. Use this screen to evaluate if the inventory adequately supports client needs within the wireless network radio coverage area.

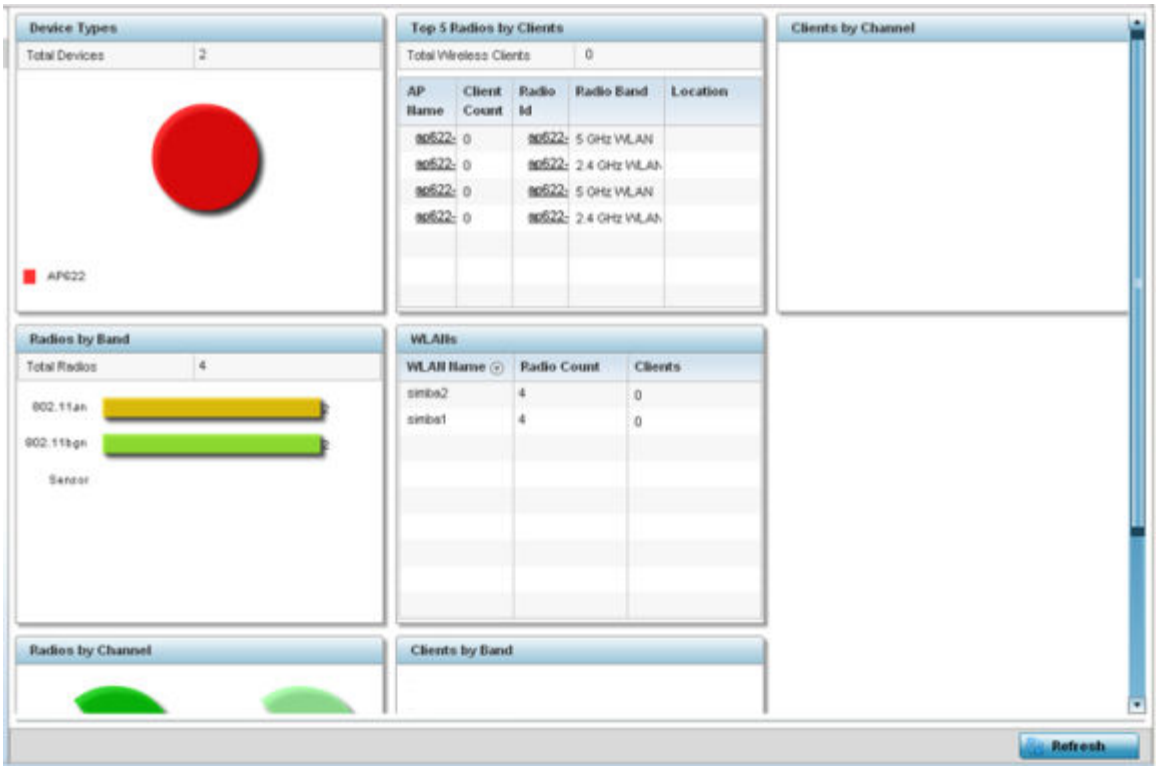
To display RF Domain inventory statistics:

1 Select the **Statistics → System** menu from the Web UI.
2 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

3 Select **Inventory** from the RF Domain menu.

The **Inventory** screen displays.




4 Review the different fields displayed on the **RF Domain > Inventory** screen:

- Device Types - Displays the total members in the RF Domain. The exploded pie chart depicts the distribution of RF Domain members by controller, service platform and AP model type.
- Radios by Band - Displays the total number of radios using 802.11an and 802.11bgn bands within the RF Domain. The number of radios designated as sensors is also represented, to reflect available sensor resources for intrusion detection.
- Radios by Channel - Displays the radio channels utilized by RF Domain member devices in two separate charts. One chart displays for 5 GHz channels and the other for 2.4 GHz channels
- Top 5 Radios by Clients - Refer the following table, which displays the highest 5 performing wireless clients connected to RF Domain members:

| | |
|---|---|
| Total Wireless Clients | Displays the total number of clients connected to RF Domain members. |
| AP Name | Displays the clients connected and reporting APs. The AP's name displays as a link that can be clicked to display AP data in greater detail. |
| Client Count | Displays the number of connected clients to each listed RF Domain member AP. |
| Radio | Displays each radio's administrator defined hostname and its radio designation (radio 1, radio 2 etc.). |
| Radio Band | Displays each client's operational radio band. |
| Location | Displays system assigned deployment location for the client. |

- WLANs - Refer to this table to review RF Domain WLAN, radio and client utilization. Use this information to help determine whether the WLANs within this RF Domain have an optimal radio and client utilization.

- Clients by Band - This bar graph displays the total number of RF Domain member clients by their IEEE 802.11 radio type.
- Clients by Channel - This pie charts displays the channels used by RF Domain member clients using 5GHz and 2.4GHz radios.

5 Periodically select **Refresh** to update the contents of the screen to their latest values.

## Devices

The Devices screen displays RF Domain member devices as links that can be selected to troubleshoot members in greater detail. Each device is listed with its factory encoded MAC address, connected client count, radio utilization and network IP address.

To display RF Domain device statistics:

1 Select the **Statistics** menu from the Web UI.

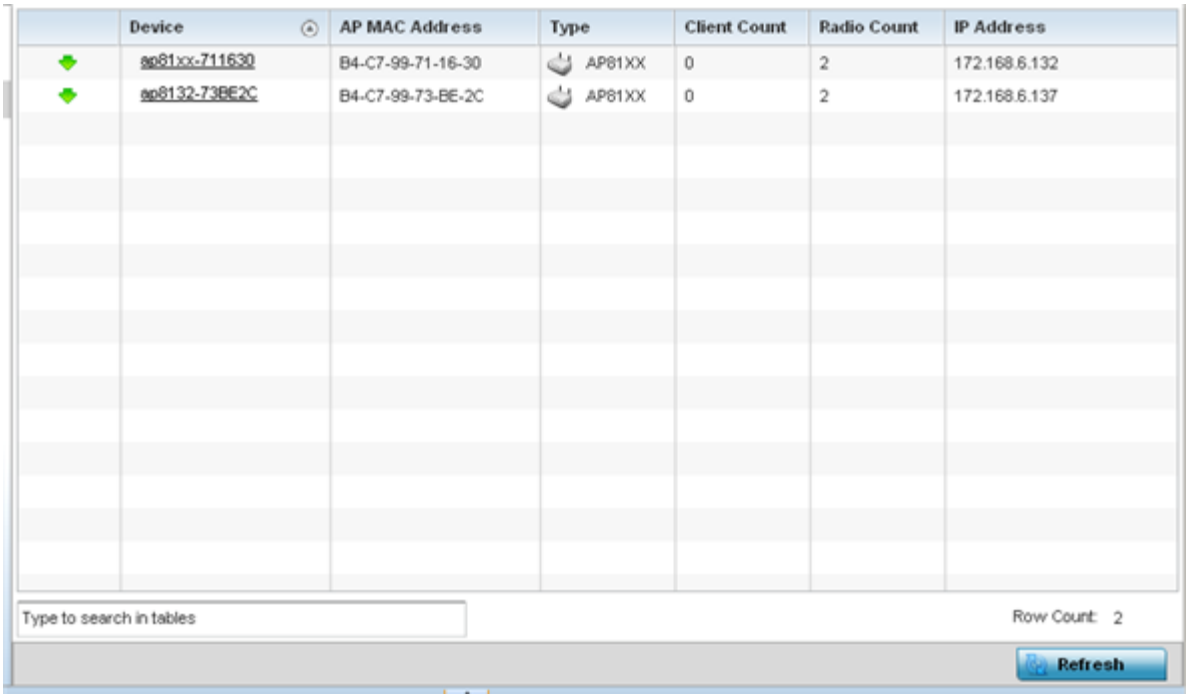
2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Devices** from the RF Domain menu.




5 Refer to the following table for information available on the Devices screen:

| | |
|---|---|
| Access Point | Displays the system assigned name of each AP that is a member of the RF Domain. The name displays as a link that you can select to view configuration and network address information in greater detail. |
| AP MAC Address | Displays each AP's factory encoded MAC address as its hardware identifier. |
| Type | Displays each AP's model type. |
| Client Count | Displays the number of clients connected with each listed AP. |
| Radio Count | Displays the number of radios on each listed device. The number of radios per AP varies with the AP model type. For example, AP 6522, AP 6562, AP 7161, AP-7612 and AP-8163 models have two radios. Where as, AP-8432 and AP-8533 model have three radios. |
| IP Address | Displays the IP address each listed AP is using a network identifier. |

6 Periodically click **Refresh** to update the contents of the screen to their latest values.

## AP Detection

The **AP Detection** screen displays information about detected APs that are not members of the selected RF Domain but have been detected within the network's device radio coverage area. They could be authorized devices or potential rogue devices requiring administration.

To view device information on detected access points:

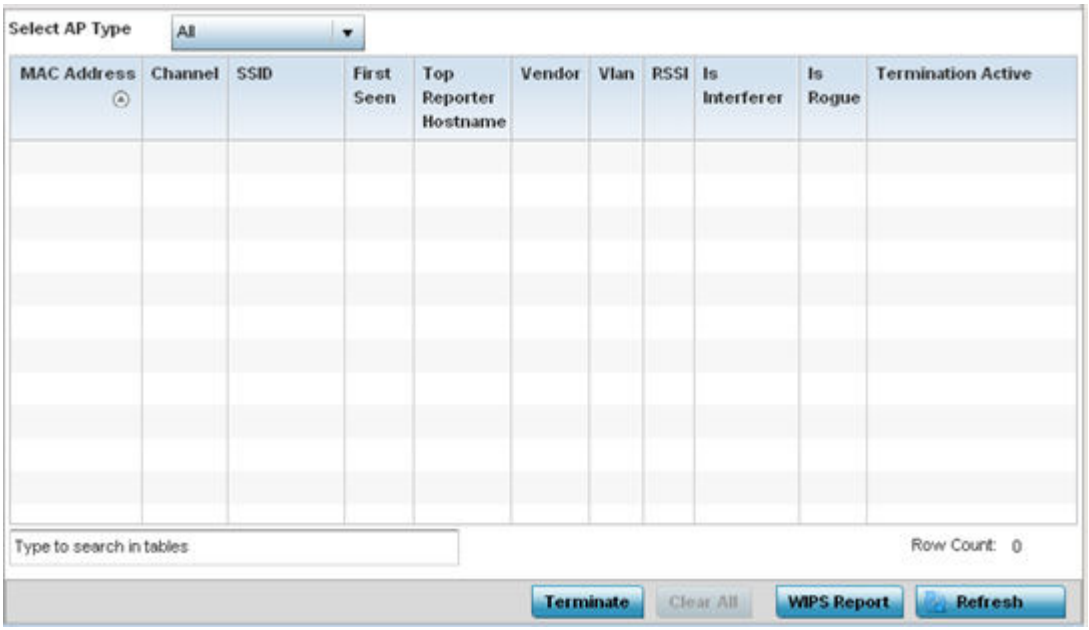
1 Go to **Statistics** → **System**.

2 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

3 Select **AP Detection** from the RF Domain menu.

The AP Detection screen displays.




4 Refer the following table for AP Detection related information:

| | |
|---|---|
| Select AP Type | Displays detected AP information based on the option selected form the drop-down menu. The options are: **All**, **Rogue**, **Interferer**, and **Termination Active**. |
| MAC Address | Displays the hardware encoded MAC address of each listed AP detected by a RF Domain member device. The MAC address is set at the factory and cannot be modified via the management software. The MAC address displays as a link that you can select to display RF Domain member device information in greater detail. |
| Channel | Displays the channel of operation used by the detected AP. The channel must be utilized by both the AP and its connected client and be approved for the target deployment country. This is necessary to designate the deployment as legal under FCC guidelines. |
| SSID | Displays the *Service Set ID* (SSID) of the network to which the detected AP belongs. |
| First Seen | Provides a time stamp when the detected AP was first seen by a RF Domain member device. |
| Top Reporter Hostname | Lists the administrator-assigned hostname of the top performing RF Domain member detecting the listed AP MAC address. Consider this top performer the best resource for information on the detected AP and its potential threat. |
| Vendor | Lists the manufacturer of the detected AP as an additional means of assessing its potential threat to the members of this RF Domain and its potential for interoperability with RF Domain device members. |
| VLAN | Lists the numeric VLAN ID (virtual interface) the detected AP was seen on by members of this RF Domain. |
| RSSI | Displays the *Received Signal Strength Indicator* (RSSI) of the detected AP. Use this variable to help determine whether a device connection would improve network coverage or add noise. |
| Is Interferer | Lists whether the detected device exceeds the administrator defined RSSI threshold (from -100 to -10 dBm) determining whether a detected AP is classified as an interferer. |
| Is Rogue | Displays whether the detected device has been classified as a rogue device whose detection threatens the interoperation of RF Domain member devices. |
| Termination Active | Lists whether Air Termination is active and applied to the detected AP. Air termination lets you terminate the connection between your WLAN and any AP or client associated with it. If the rogue device is an AP, all client association with the AP are removed. If the rogue device is a client, its connection with the AP is terminated. Note, Air Termination is disabled by default. |

5 Click **Terminate** to remove the selected AP from RF Domain membership.

6 Click **Clear All** to reset the statistics counters to zero and begin a new data collection.

7 Click WIPS Report to launch a sub-screen to save a WIPS report (in PDF format) to a specified location.

Note

You are recommended to capture RF Domain member AP's client connection terminations in a format that can be archived externally.

8 Click **Refresh** to update the statistics counters to their latest values.

## Device Upgrade

The Device Upgrade screen displays information about devices, within the selected RF Domain, receiving updates and devices performing updates. Use this screen to gather version data, install firmware images, boot an image and upgrade status.

To view the device upgrade statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

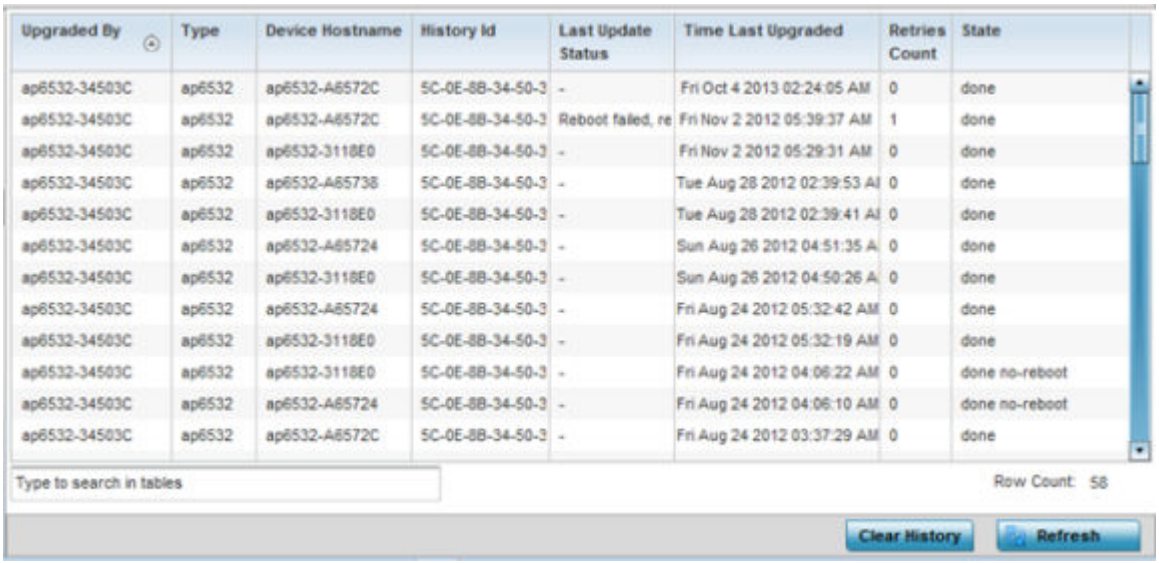
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Device Upgrade** from the RF Domain menu.

The Device Upgrade screen displays.




5 Refer the following table for Device Upgrade related information:

| | |
|---|---|
| Upgraded By | Lists the name of the device performing an update on behalf of a RF Domain member peer device. |
| Type | Displays the model of the device receiving an update. With introduction of heterogeneous adoption, it is no loner necessary that the updating access point must be of the same model as the access point receiving the update. For more information on heterogeneous adoption, click here. |
| Device Hostname | Lists the administrator-assigned hostname of each device receiving an update from a RF Domain member. |
| History ID | Lists the RF Domain member device's MAC address along with a history ID appended to it for each upgrade operation. |
| Last Update Status | Displays the last status message from the RF Domain member device performing the upgrade operation. |
| Time Last Upgraded | Displays the date and time of the last firm ware image upgrade operation. |
| Retries Count | Lists the number of retries needed for each listed RF Domain member update operation. |
| State | Lists whether the upgrade operation is completed, in-progress, failed or whether an update was made without a device reboot. |

6 Click **Clear History** to remove the upgrade records for RF Domain member devices.
7 Click **Refresh** to update the screen's statistics counters to their latest values.

## Wireless Clients

The Wireless Clients screen displays device information for wireless clients connected to RF Domain member APs. Review this content to determine whether a client should be removed from AP association within the selected RF Domain.

To review a RF Domain's connected wireless clients:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

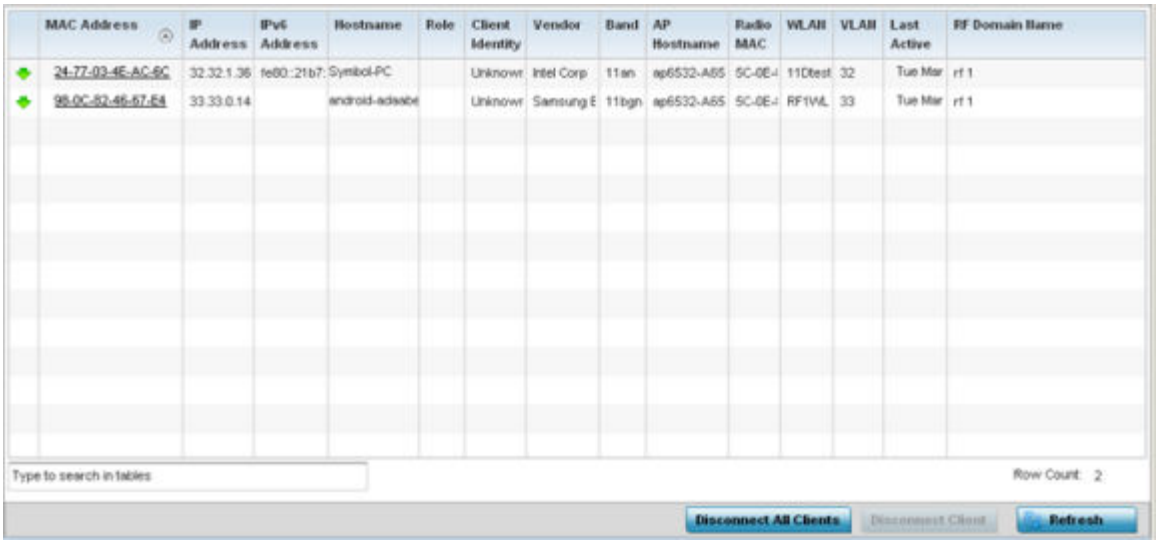
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select Wireless Clients from the RF Domain menu.

The Wireless Clients screen displays.




5 Refer the following table for Wireless Clients related information:

| | |
|---|---|
| MAC Address | Displays the hostname (MAC address) of each listed wireless client. This address is hard-coded at the factory and can not be modified. The hostname address displays as a link that you can select to view client configuration and network address information in greater detail. |
| IP Address | Displays the current IP address the wireless client is using for a network identifier. |
| IPv6 Address | Displays the current IPv6 formatted IP address a listed wireless client is using as a network identifier. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |

| | |
|---|---|
| Hostname | Displays the unique administrator-assigned hostname when the client connection was defined. |
| Role | Lists the role assigned to each controller, service platform or AP managed client. |
| Client Identity | Lists the client's operating system identity (Android, Windows, etc.). |
| Vendor | Displays the manufacturer of each listed client as a means of assessing its support capabilities with the WiNG managed wireless infrastructure. |
| Band | Lists the 2.4 or 5 GHz radio band the listed client is currently utilizing with its connected access point within the RF Domain. |
| AP Hostname | Displays administrator-assigned hostname of the AP reporting client stats to RF Domain member devices. |
| Radio MAC | Displays the hardware-encoded MAC address of the AP radio to which the client is currently connected within the RF Domain. |
| WLAN | Displays the name of the WLAN the wireless client is currently using for its AP interoperation within the RF Domain. |
| VLAN | Displays the VLAN ID the client's connected AP has defined for use as a virtual interface. |
| Last Active | Displays the last detected transmit and receive activity for the listed client within the WiNG managed device radio coverage area. |
| RF Domain Name | Lists each client's RF Domain membership as defined by its connected access point and associated controller or service platform. |

6 Click **Disconnect All Clients** to terminate each listed client's connection and RF Domain membership.

7 Select a specific client MAC address, and click the **Disconnect Client** to terminate this client's connection and RF Domain membership.

8 Periodically click **Refresh** button to update the statistics counters to their latest values.

## Wireless LANs

The Wireless LANs screen displays the name, network identification and radio quality information for the WLANs currently being utilized by RF Domain members.

To view wireless LAN statistics for RF Domain members:

1 Select the Statistics menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

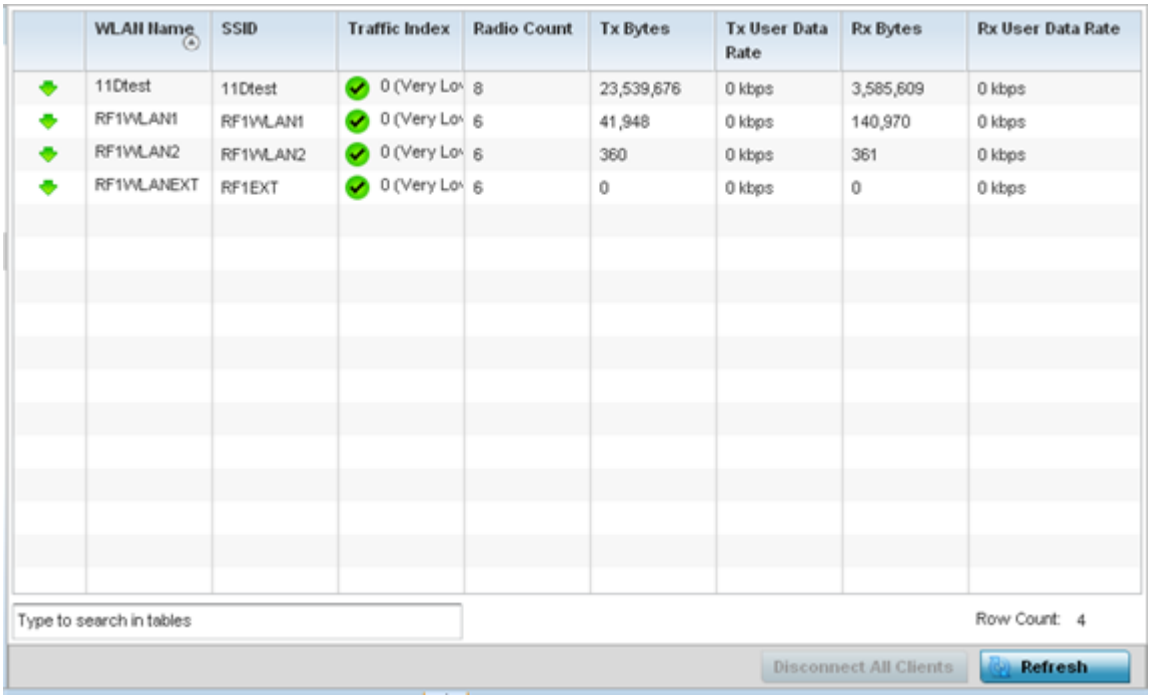
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select Wireless LANs from the RF Domain menu.

The Wireless LANs screen displays.




5 Refer the following table for Wireless LANs related information:

| | |
|---|---|
| WLAN Name | Displays the name assigned to the WLAN upon its creation within the controller, service platform managed or AP network. |
| SSID | Displays the SSID assigned to the WLAN. |
| Traffic Index | Displays the traffic utilization index of each listed WLAN, which measures how efficiently the traffic medium is used. It's defined as the percentage of current throughput relative to the maximum possible throughput. Traffic indices are:<br>• **0 – 20** - (very low utilization)<br>• **20 – 40** - (low utilization)<br>• **40 – 60** - (moderate utilization)<br>• **60 and above** - (high utilization) |
| Radio Count | Displays the number of radios deployed in each listed WLAN within this RF Domain. Use this information to assess each WLAN's client support capabilities in respect to the number of radio's available and their operational band. |
| Tx Bytes | Displays the average number of packets (in bytes) sent on each listed RF Domain member WLAN. |
| Tx User Data Rate | Displays the average data rate per user for packets transmitted on each listed RF Domain member WLAN. |
| Rx Bytes | Displays the average number of packets (in bytes) received on each listed RF Domain member WLAN. |
| Rx User Data Rate | Displays the average data rate per user for packets received on each listed RF Domain member WLAN. |

6 Click **Disconnect All Clients** to terminate all client's WLAN membership.

7 Click **Disconnect Client** to terminate a selected client's WLAN membership.

8 Periodically click **Refresh** to update the statistics counters to their latest values.

## Radios

The **Radio** screens displays information on RF Domain member access point radios. This information in reported as collective set of data from each radio deployed device supporting client traffic requirements within the RF Domain. Use these screens to troubleshoot radio issues negatively impacting RF Domain performance.

The **RF Domain > Radio** option has the following sub-menus:

- Status
- RF Statistics
- Traffic Statistics

### *Radios Status*

The **Status** screen displays network address, access point model, operational channel and client device status information for detected RF Domain member device radios serving and client support resources for the selected RF Domain.

To view the RF Domain radio statistics:

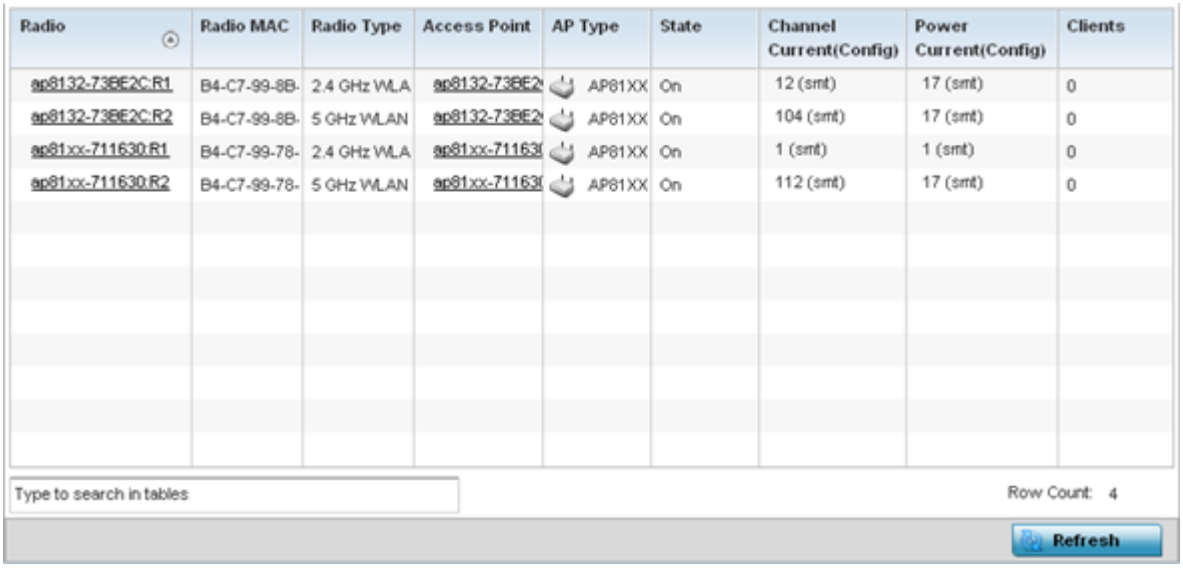
1 Go to **Statistics → System** menu from the Web UI.

2 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

3 Expand **Radios** from the RF Domain menu.

The **Radios → Status** screen displays by default.




4 Refer the following table for **Radio Status** information:

| | |
|---|---|
| Radio | Displays the name assigned to each listed RF Domain member access point radio. Each name displays as a link that you can be select to view radio information in greater detail. |
| Radio MAC | Displays the MAC address as a factory-set, numerical value hard coded for each listed RF Domain member AP radio. |
| Radio Type | Defines whether the radio is operating within the 2.4 or 5 GHz radio band |
| Access Point | Displays the user assigned name of the RF Domain member access point to which the radio resides. |
| AP Type | Lists the model type of each listed RF Domain member AP. |
| State | Displays the radio's current operational state. |
| Channel Current (Config) | Displays the current channel each listed RF Domain member AP radio is broadcasting on. |
| Power Current (Config) | Displays the current power level the radio is using for transmissions. |
| Clients | Displays the number of clients currently connected to each listed RF Domain member AP radio. Supported models can manage up to 256 clients per radio. |

5 Click **Refresh** to update the statistics counters to their latest values.

### *Radio RF Statistics*

The RF Statistics screen lists signal, noise ratio, transmit and receive, error and retry information for RF Domain member access point radios. Individual radios can be selected as needed to display (and troubleshoot) information specific to that RF Domain member radio resource.

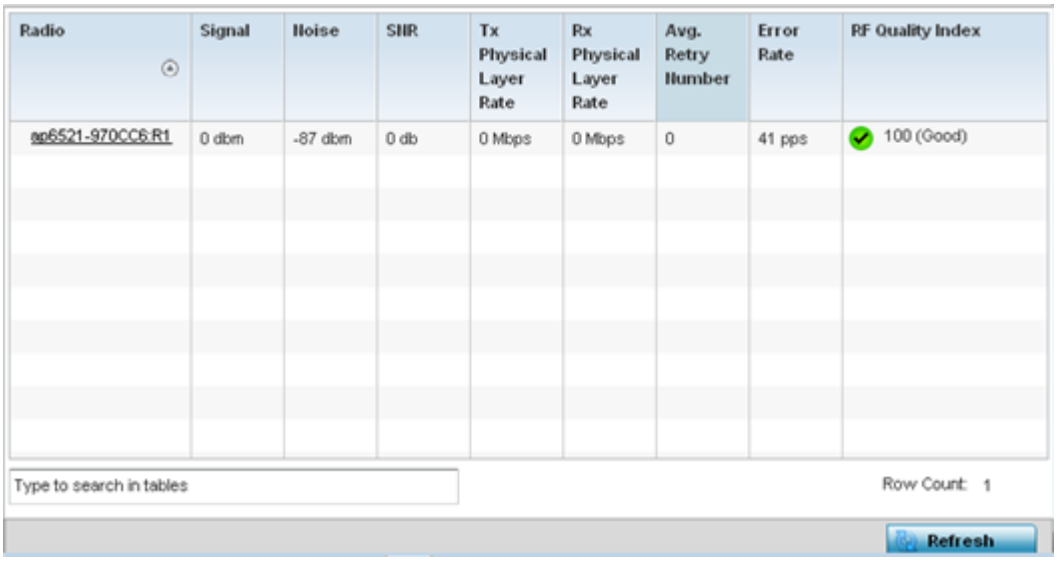
To view the RF Domain radio statistics:

1 Select the **Statistics → System** menu from the Web UI.
2 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

3 Expand **Radios** and select **RF Statistics**.

The RF Statistics screen displays.




4 Refer the following table for the **Radio RF Statistics** information:

| | |
|---|---|
| Radio | Displays the name assigned to each listed RF Domain member radio. Each name displays as a link that can be selected to display individual radio information in greater detail. |
| Signal | Displays the power of listed RF Domain member radio signals in dBm. |
| Noise | Lists the level of noise (in - X dbm format) reported by each listed RF Domain member AP. |
| SNR | Displays the *signal to noise ratio* (SNR) of each listed RF Domain member radio. |
| Tx Physical Layer Rate | Displays the data transmit rate for each RF Domain member radio's physical layer. The rate is displayed in Mbps. |
| Rx Physical Layer Rate | Displays the data receive rate for each RF Domain member radio's physical layer. The rate is displayed in Mbps. |
| Avg Retry Number | Displays the average number of retries for each RF Domain member radio. |
| Error Rate | Displays the average number of retries per packet. A high number indicates possible network or hardware problems. |
| RF Quality Index | Displays an integer (and performance icon) that indicates the overall RF performance for each listed radio. The RF quality indices are:<br>• **0 – 50** - (Poor)<br>• **50 – 75** - (Medium)<br>• **75 – 100** - (Good) |

5 Periodically click **Refresh** to update the contents of the screen to their latest values

### *Radio Traffic Statistics*

The **Traffic Statistics** screen displays transmit and receive data as well as data rate and packet drop and error information for RF Domain member radios. Individual RF Domain member radios can be selected and to information specific to that radio as troubleshoot requirements dictate.

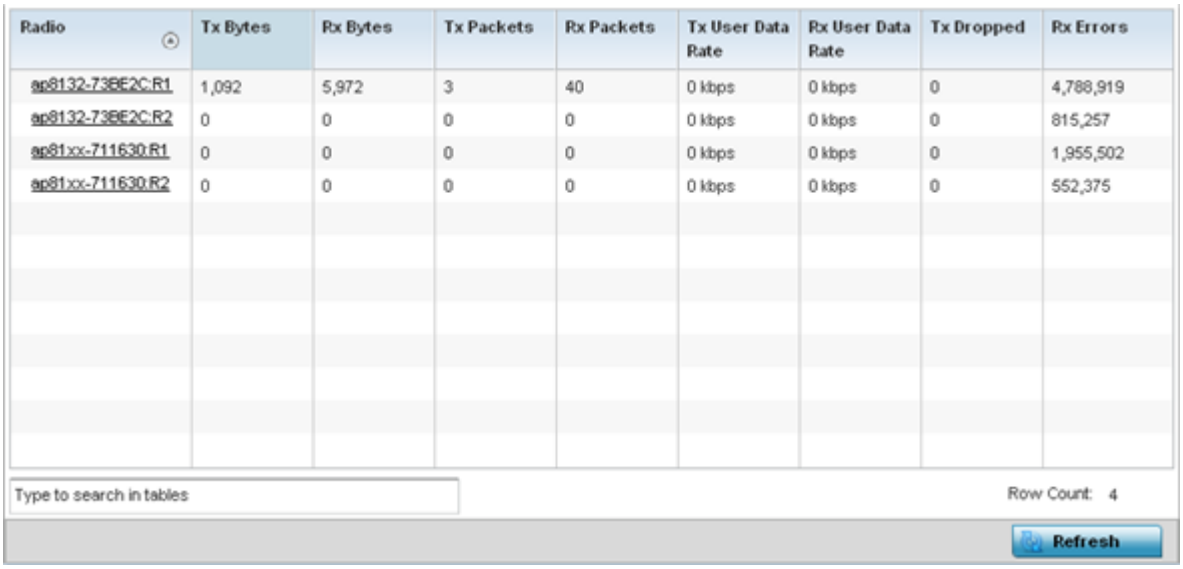
To view RF Domain member AP radio traffic statistics:

1 Go to **Statistics → System**.
2 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

3 Expand **Radios** and select **Traffic Statistics**.

The **Radio Traffic Statistics** screen displays.




4 Refer the following table for **Radio Traffic Statistics** information:

| | |
|---|---|
| Radio | Displays the name assigned to each listed RF Domain member access point radio. Each name displays as a link that you can select to view individual radio information in greater detail. |
| Tx Bytes | Displays the total number of bytes transmitted by each RF Domain member AP radio. This includes all user data as well as any management overhead data. |
| Rx Bytes | Displays the total number of bytes received by each RF Domain member AP radio. This includes all user data as well as any management overhead data. |
| Tx Packets | Displays the total number of packets transmitted by each RF Domain member AP radio. This includes all user data as well as any management overhead packets. |
| Rx Packets | Displays the total number of packets received by each RF Domain member AP radio. This includes all user data as well as any management overhead packets. |
| Tx User Data Rate | Displays the rate (in kbps) user data is transmitted by each RF Domain member AP radio. This rate only applies to user data and does not include any management overhead. |
| Rx User Data Rate | Displays the rate (in kbps) user data is received by each RF Domain member AP radio. This rate only applies to user data and does not include any management overhead. |
| Tx Dropped | Displays the total number of packets dropped by each RF Domain member AP radio during transmission. This includes user data as well as management overhead packets. |
| Rx Errors | Displays the total number of packets containing errors, received by each RF Domain member AP radio. |

5 Click **Refresh** to update the statistics counters to their latest values.

## Bluetooth

The AP7602, AP7612, AP7632, AP7662, AP8432 and AP8533 model access points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network.

These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

AP-8432 and AP-8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone- URL beacons. The access point's Bluetooth radio sends non-connectable, undirected LE *(low-energy)* advertisement packets on a periodic basis. These advertisement packets are short, and they are sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. Portions of the advertising packet are still customizable, however.

**Note**
The WiNG 7.1 release does not support Bluetooth on AP505 and AP510 model access points. This feature will be supported in future releases.

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

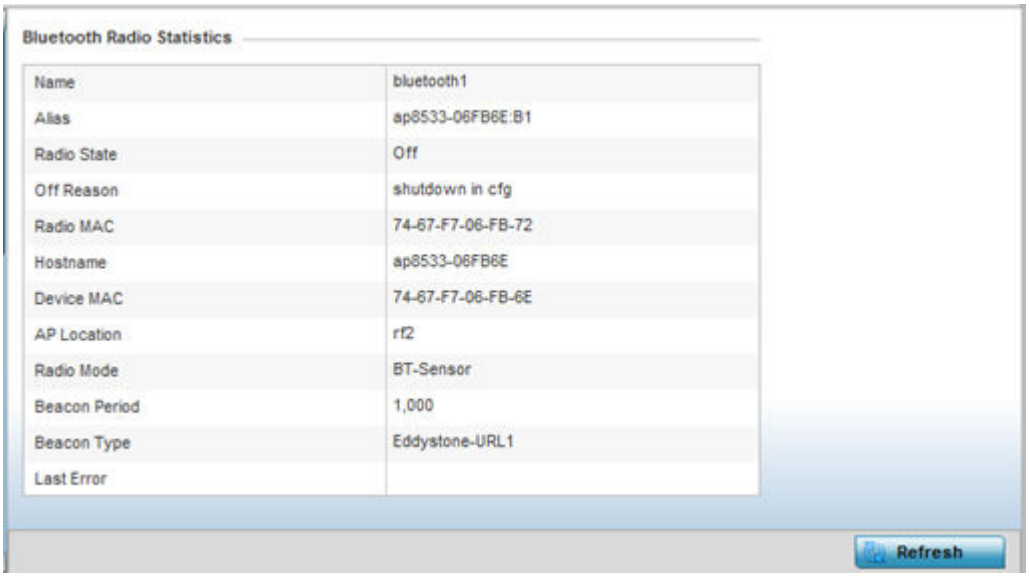
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Click **Bluetooth**.

The **Statistics** → **RF Domain** → **Bluetooth** screen displays.




5 Refer the following table for Bluetooth related information:

| | |
|---|---|
| Name | Lists the administrator assigned name of the access point's Bluetooth radio. |
| Alias | If an alias has been defined for the AP it is listed here. The alias value is expressed in the form of <hostname>: B<Bluetooth_radio_number>. If the administrator has defined a hostname for the AP, it is used in place of the AP's default hostname. |
| Radio State | Displays the current operational state (On/Off) of the Bluetooth radio. |
| Off Reason | If the Bluetooth radio is offline, this field states the reason. |
| Radio MAC | Lists the Bluetooth radio's factory-encoded MAC address serving as this device's hardware identifier on the network. |
| Hostname | Lists the AP's hostname as its network identifier. |
| Device MAC | Lists the AP's factory-encoded MAC address serving as this device's hardware identifier on the network. |
| AP Location | Lists the AP's administrator-assigned deployment location. |
| Radio Mode | Lists an access point's Bluetooth radio functional mode as either **`btsensor`** or **`le-beacon`**. |
| Beacon Period | Lists the Bluetooth radio's beacon transmission period from 100 -10,000 milliseconds. |
| Beacon Type | Lists the type of beacon currently configured. |
| Last Error | Lists descriptive text on any error that is preventing the Bluetooth radio from operating. |

6 Click **Refresh** to update the statistics counters to their latest values.

## Mesh

Mesh networking provides users wireless access to broadband applications anywhere (even in a moving vehicle). Initially developed for secure and reliable military battlefield communications, mesh technology supports public safety, public access and public works. Mesh technology reduces the expense of wide-scale networks, by leveraging Wi-Fi enabled devices already deployed.

Note
The WiNG 7.1 release does not support MeshConnex on AP505 and AP510 model access points. This feature will be supported in future releases.

To view Mesh statistics for RF Domain member mesh node connected clients:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

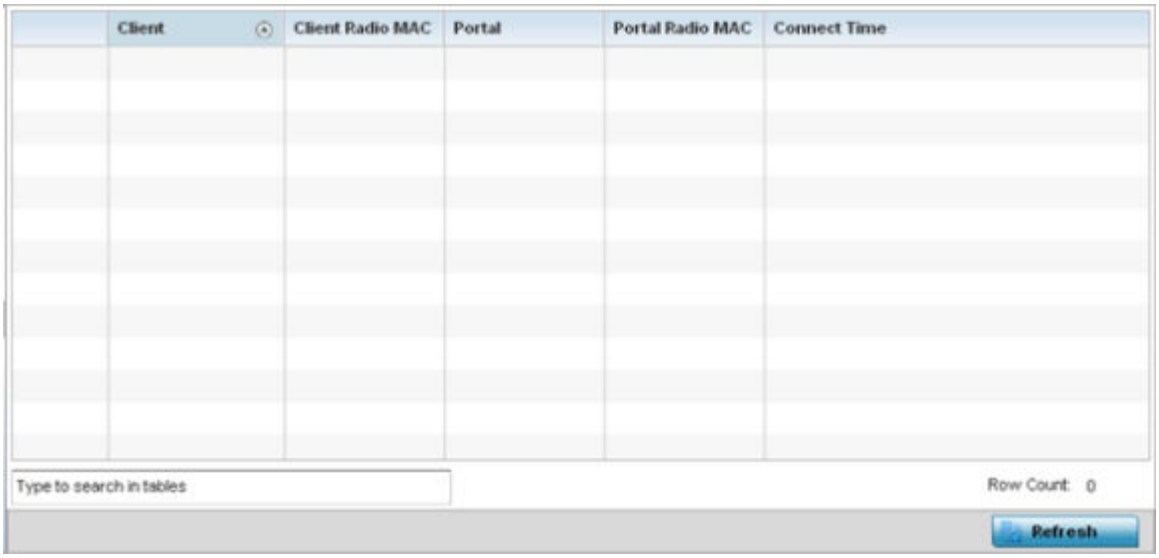
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Click **Mesh**.

The Mesh screen displays.




5 Refer the following table for **Mesh** statistics information:

| | |
|---|---|
| Client | Displays the administrator-defined hostname for each mesh client connected to a RF Domain member AP radio. |
| Client Radio MAC | Displays the hardware-encoded MAC address for each mesh client connected to a RF Domain member AP radio. |
| Portal | Displays a numerical portal Index ID for the each mesh client connected to a RF Domain member AP radio. |
| Portal Radio MAC | Displays the hardware encoded MAC address for each radio in the RF Domain's mesh network. |
| Connect Time | Displays the total connection time for each listed client within the RF Domain's mesh network. |

6 Click **Refresh** to update the statistics counters to their latest values.

## Mesh Point

Mesh networking provides users wireless access to broadband applications anywhere (even in a moving vehicle). Initially developed for secure and reliable military battlefield communications, mesh technology supports public safety, public access and public works. Mesh technology reduces the expense of wide-scale networks, by leveraging Wi-Fi enabled devices already deployed.

*Mesh points* are APs dedicated to mesh network support. Mesh points capture and disseminate their own data and serve as a relay for other nodes.

Note
The WiNG 7.1 release does not support MeshConnex on AP505 and AP510 model access points. This feature will be supported in future releases.

The **RF Domain > Mesh Point** option has the following sub-menus:

- MCX Geographical View on page 942.
- MCX Logical View on page 943.

- Device Type on page 944.
- Device Brief Info on page 949.
- Device Data Transmit on page 955.

*MCX Geographical View*

The **MCX Geographical View** displays a map where icons of each device in the RF Domain is overlaid. This provides a geographical overview of the location of each RF Domain member device.

To display the MCX Geographic View:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

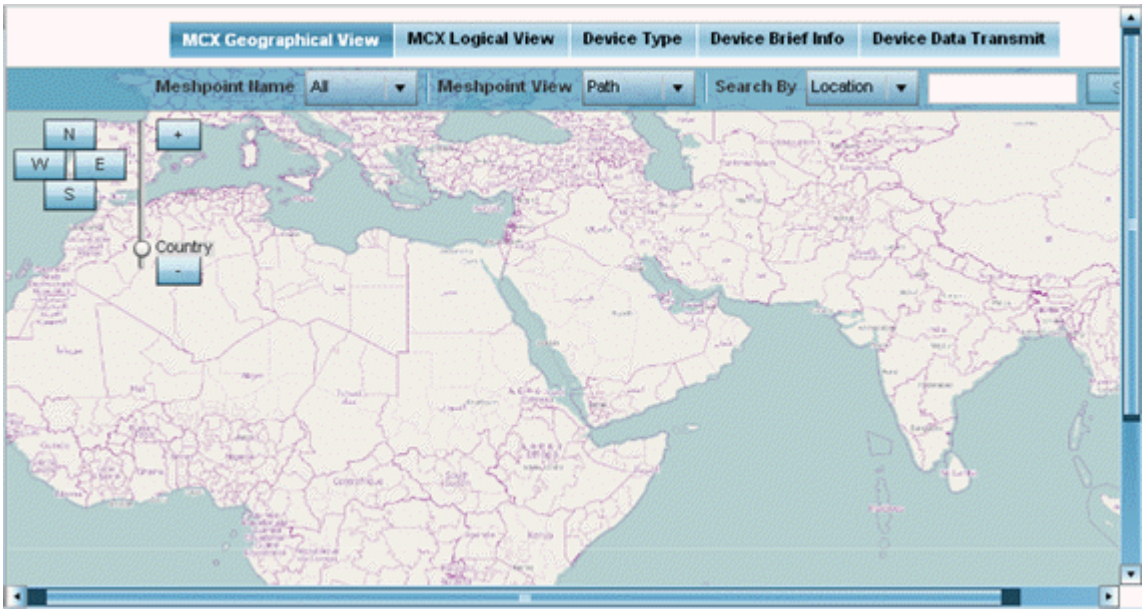
The **System** node expands to display the RF Domains created within the managed network.

3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **Mesh Point** from the RF Domain menu.

The **MCX Geographical View** screen displays by default.




This screen displays a map overlaid with icons of each device deployed within the selected RF Domain. Use this screen for an overview of geographical location of RF Domain member mesh devices.

5 Use the **N**, **W**, **E** and **S** buttons to scroll the map up, down or side-ways in the North, East, West and South directions. Use the slider next to these buttons to zoom in and out. The available fixed zoom levels are **`World`**, **`Country`**, **`State`**, **`Town`**, **`Street`** and **`House`**.
6 Use the **Meshpoint Name** drop-down menu to select the mesh point name from the list displayed. Or, select **All** to view mesh statistics for all mesh points within the selected RF Domain.
7 Use the **Meshpoint View** drop-down menu to specify the view type as either **Path** or **Neighbor**.

8 Use the **Search By** drop-down menu to specify the search range as: **`Location`**, **`Device MAC`** or **`Hostname`**.

9 Based on the **Search by** option specified, enter the search criteria in the **Search** field, and click **Search**.

10 Click **Maximize** for full-screen view.

11 Periodically, click **Refresh** to update the status of the screen.

### *MCX Logical View*

The MCX Logical View screen provides a logical representation of mesh point statistics.

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

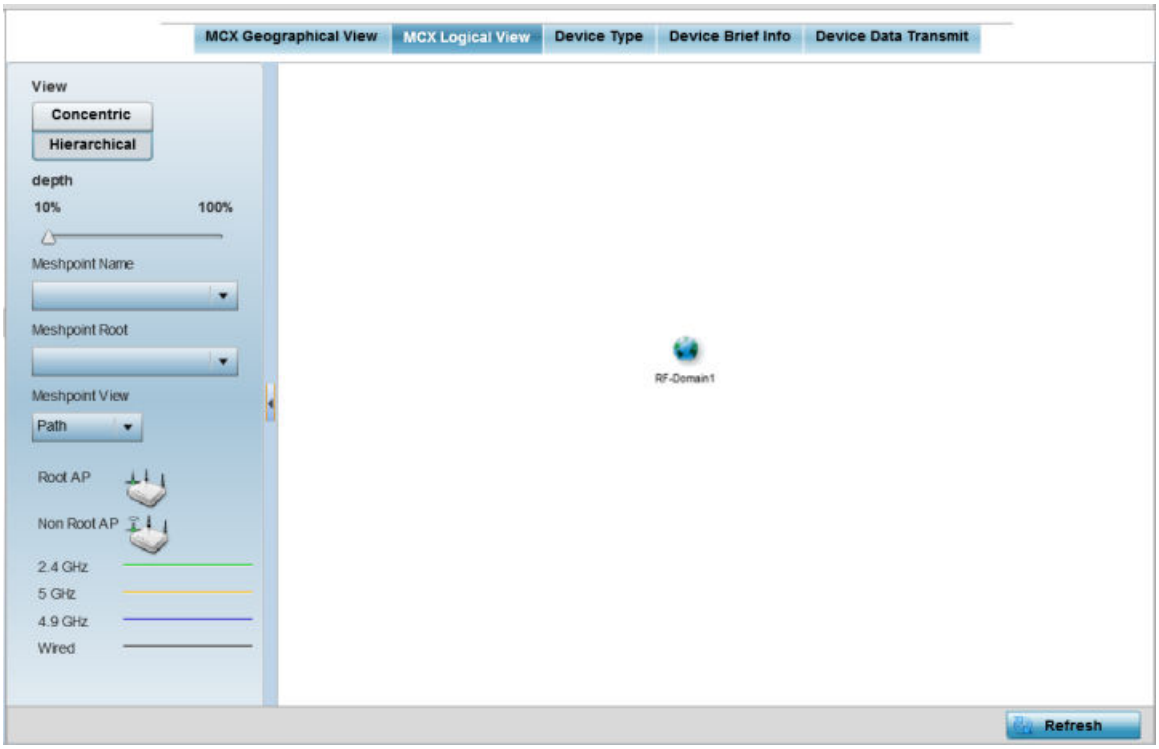
The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Mesh Point** from the RF Domain menu.

The MCX Geographical View screen displays by default.

5 Click **MCX Logical View**.

The MCX Logical View screen displays.




This screen has two panes. The left-hand pane provides filter options to help you define the display format. The right-hand pane displays mesh statistics based on the filters specified by you in the left-hand pane.

In the left-hand pane:

6 Specify the View format as **Concentric** or **Hierarchical** .

The Concentric view displays the mesh as a concentric arrangement of devices, with the mesh's root node at the centre and the other mesh devices arranged in circles around it.

The Hierarchical view displays the mesh's root node at the top of the mesh tree, and the relationship of the mesh nodes are displayed as such.

7 Use the **Meshpoint Name** drop-down menu to select the mesh point. The graphical representation of the selected mesh point is displayed in the right-hand view area.

8 Use the **Meshpoint Root** drop-down to select the mesh root. Or, select **All Roots**.

9 To further refine the display, use the **Meshpoint View** drop-down menu to specify the view type as either **Path** or **Neighbor**.

10 Periodically click **Refresh** to update the status of the screen.

*Device Type*

To view mesh point statistics for RF Domain member access points and their connected clients:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

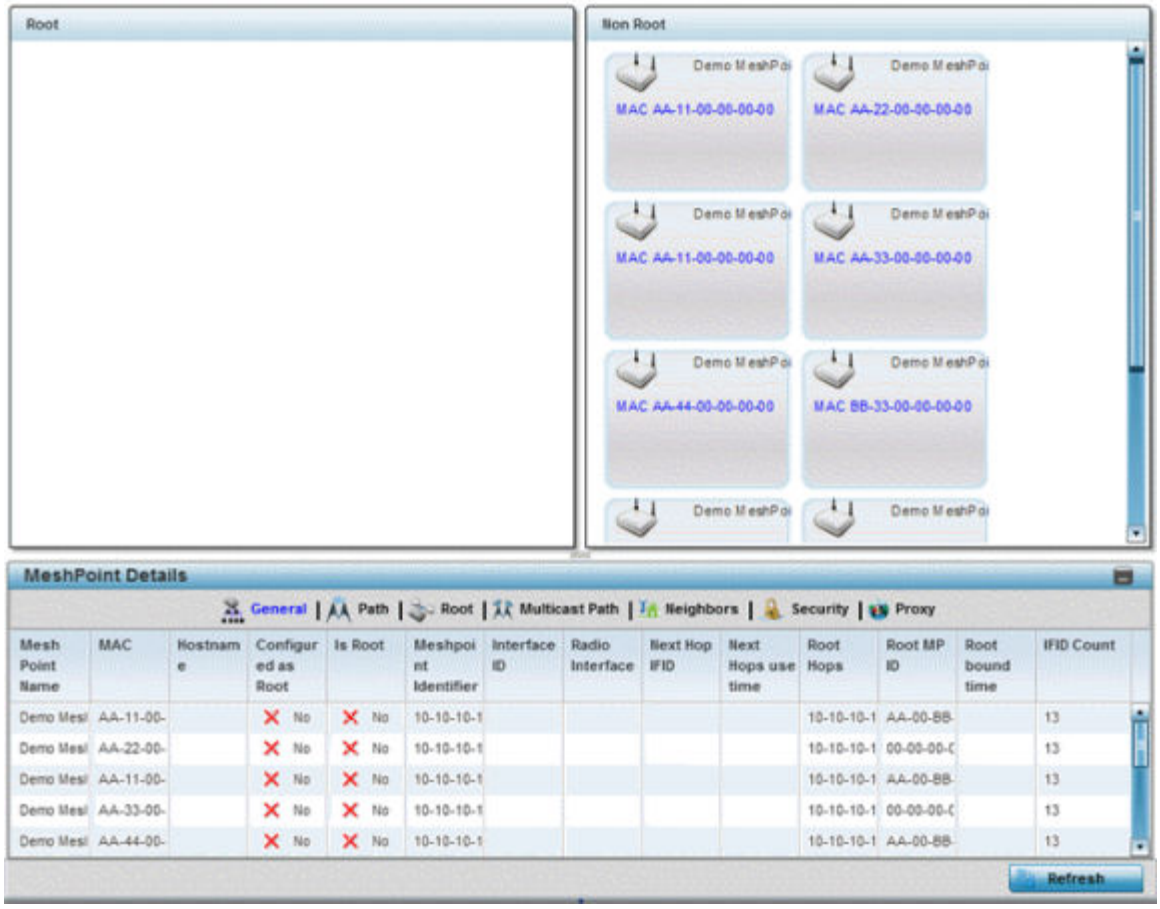
The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Mesh Point** from the RF Domain menu.

The MCX Geographical View screen displays by default.

5 Click **Device Type**.

The Device Type screen displays by default.




This screen has the following elements:

- The Root field - the top, left-hand pane that displays the Mesh ID and MAC Address of the configured root mesh points in the RF Domain.
- The Non Root field - the top, right-hand pane that displays the Mesh ID and MAC Address of all configured non-root mesh points in the RF Domain. displays the Mesh ID and MAC Address of all configured non-root mesh points in the RF Domain.
- The MeshPoint Details table- the bottom pane that displays the following tabs: General, Path, Root, Multicast Path, Neighbors, Security and Proxy. Refer to the following:

6 Click the **General** tab.

Refer the following table for the General tab information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| MAC | Displays the MAC Address of each configured mesh point in the RF Domain. |
| Hostname | Displays the administrator assigned hostname for each configured mesh point in the RF Domain. |
| Configured As Root | Indicates whether a mesh point is configured to act as a root device. (**Yes**/**No**). |
| Is Root | A root mesh point is defined as a mesh point connected to the WAN and provides a wired backhaul to the network (**Yes**/**No**). |

| | |
|---|---|
| Meshpoint Identifier | The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration. |
| Interface ID | The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces. |
| Next Hop IFID | Lists the ID of the interface on which the next hop for the mesh network can be found. |
| Next Hops Use Time | Lists the time when the next hop in the mesh network was last utilized. |
| Root Hops | Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out. |
| Root MP ID | Displays the ID of the root device for this mesh point. |
| Root Bound Time | Displays the duration this mesh point has been connected to the mesh root. |
| IFID Count | Displays the number of *Interface IDs* (IFIDs) associated with all the configured mesh points in the RF Domain. |

7 Click the **Path** tab.

Refer the following table for detailed information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a Mesh Point ID. |
| Next Hop IFID | The Interface ID of the mesh point that traffic is being directed to. |
| Is Root | A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (**Yes**/**No**). |
| MiNT ID | Displays the MiNT Protocol ID for the global mint area identifier. This area identifier separates two overlapping mint networks and need only be configured if the administrator has two mint networks that share the same packet broadcast domain. |
| Hops | Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out. |
| Mobility | Displays whether the mesh point is a mobile or static node. Displays **True** when the device is mobile and **False** when the device is not mobile. |
| Metric | A measure of the quality of the path. A lower value indicates a better path. |
| State | Indicates whether the path is currently **Valid** of **Invalid**. |
| Binding | Indicates whether the path is bound or unbound. |
| Timeout | The timeout interval in milliseconds. The interpretation this value will vary depending on the value of the state. |
| Sequence | The sequence number also known as the destination sequence number. It is updated whenever a mesh point receives new information about the sequence number from *RREQ*, *RREP*, or *RERR* messages that may be received related to that destination. |

8 Click the **Root** tab.

Refer the following table for the Root tab information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Recommended | Displays the root that is recommended by the mesh routing layer. |

| | |
|---|---|
| Root MPID | The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration. |
| Next Hop IFID | The IFID of the next hop. The IFID is the MAC Address on the destination device. |
| Radio Interface | This indicates the interface that is used by the device to communicate with this neighbor. The values are **2.4** and **5.8**, indicating the frequency of the radio that is used to communicate with the neighbor. |
| Bound | Indicates whether the root is bound or unbound. |
| Metric | Displays the computed path metric between the neighbor and their root mesh point. |
| Interface Bias | This field lists any bias applied because of the Preferred Root Interface Index. |
| Neighbor Bias | This field lists any bias applied because of the Preferred Root Next-Hop Neighbor IFID. |
| Root Bias | This field lists any bias applied because of the Preferred Root MPID. |

9 Click the **Multicast Path** tab.

Refer the following table for the Multicast Path tab information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Subscriber Name | The identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration. |
| Subscriber MPID | Lists the subscriber ID to distinguish between other mesh point neighbor devices in the RF Domain. |
| Group Address | Displays the MAC address used for the Group in the mesh point. |
| Timeout | The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is **Init** or **In Progress**, the timeout duration has no significance. If the state is **Enabled**, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is **Failed**, the timeout duration is the amount of time after which the system will retry. |

10 Click the **Neighbors** tab.

Refer the following table for the Neighbors tab information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | Displays the MeshID (MAC Address) of each mesh point in the RF Domain. |
| Neighbor MP ID | The MAC Address that the device uses to define the mesh point in the device that the neighbor is a part of. It is used to distinguish the device that is the neighbor. |
| Neighbor IFID | The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh. |
| Root MP ID | The MAC Address of the neighbor's root mesh point. |
| Is Root | A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. **Yes** if the mesh point that is the neighbor is a root mesh point or **No** if the mesh point that is the neighbor is not a root mesh point. |

| | |
|---|---|
| Mobility | Displays whether the mesh point is a mobile or static node. Displays **True** when the device is mobile and **False** when the device is not mobile. |
| Radio Interface | This indicates the interface that is used by the device to communicate with this neighbor. The values are **2.4** and **5.8**, indicating the frequency of the radio that is used to communicate with the neighbor. |
| Mesh Root Hops | The number of devices between the neighbor and its root mesh point. If the neighbor is a root mesh point, this value will be **0**. If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be **1**. Each mesh point between the neighbor and its root mesh point is counted as 1 hop. |
| Resourced | Displays whether the mesh point has been resourced or not. The Mesh Connex neighbor table can contain more neighbors than the AP supports. If the neighbor is resourced, it will take away a one of the resources for a wireless client device to be used for meshing. Displays **True** when the device is resourced and **False** when the device is not. |
| Link Quality | An abstract value depicting the quality of the mesh link between the device and the neighbor. The range is from 0 (weakest) to 100 (strongest). |
| Link Metric | This value shows the computed path metric from the device to the neighbor mesh point using this interface. The lower the number the better the possibility that the neighbor will be chosen as the path to the root mesh point. |
| Root Metric | The computed path metric between the neighbor and their root mesh point. |
| Rank | The rank is the level of importance and is used for automatic resource management.<br>• **8** – The current next hop to the recommended root.<br>• **7** – Any secondary next hop to the recommended root to has a good potential route metric.<br>• **6** – A next hop to an alternate root node.<br>• **5** – A downstream node currently hopping through to get to the root.<br>• **4** – A downstream node that could hop through to get to the root, but is currently not hopping through any node (look at authentication, as this might be an issue).<br>• **3** – A downstream node that is currently hopping through a different node to get to the root, but could potentially have a better route metric if it hopped through this node.<br>• **2** – Reserved for active peer to peer routes and is not currently used.<br>• **1** - A neighbor bound to the same recommended root but does not have a potential route metric as good as the neighbors ranked 8 and 7.<br>• **0** – A neighbor bound to a different root node.<br>• **-1** – Not a member of the mesh as it has a different mesh ID.<br>All client devices hold a rank of 3 and can replace any mesh devices lower than that rank. |
| Age | Displays the number of miliseconds since the mesh point last heard from this neighbor. |

11 Click the **Security** tab.

Refer the following table for the Security tab information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Radio Interface | This indicates the interface that is used by the device to communicate with this neighbor. The values are **2.4** and **5.8**, indicating the frequency of the radio that is used to communicate with the neighbor. |

| | |
|---|---|
| Interface ID | The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces. |
| State | Displays the Link State for each mesh point:<br>• **Init** - indicates the link has not been established or has expired.<br>• **Enabled –** indicates the link is available for communication.<br>• **Failed** - indicates the attempt to establish the link failed and cannot be retried yet.<br>• **In Progress –** indicates the link is being established but is not yet available. |
| Timeout | Displays the maximum value in seconds that the link is allowed to stay in the **In Progress** state before timing out. |
| Keep Alive | **Yes** indicates that the local MP will act as a supplicant to authenticate the link and not let it expire (if possible). **No** indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP. |

12 Click the **Proxy** tab.

Refer the following table for the Proxy tab information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Proxy Address | Displays the MAC Address of the proxy used in the mesh point. |
| Age | Displays the age of the proxy connection for each of the mesh points in the RF Domain. |
| Proxy Owner | The owner (MPID) is used to distinguish the device that is the neighbor. |
| Persistence | Displays the persistence (duration) of the proxy connection for each of the mesh points in the RF Domain. |
| VLAN | The VLAN ID used as a virtual interface with this proxy. A value of **4095** indicates that there is no VLAN ID. |

13 Periodically click **Refresh** to update the status of the screen.

*Device Brief Info*

To view mesh point statistics for RF Domain member APs and their connected clients:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

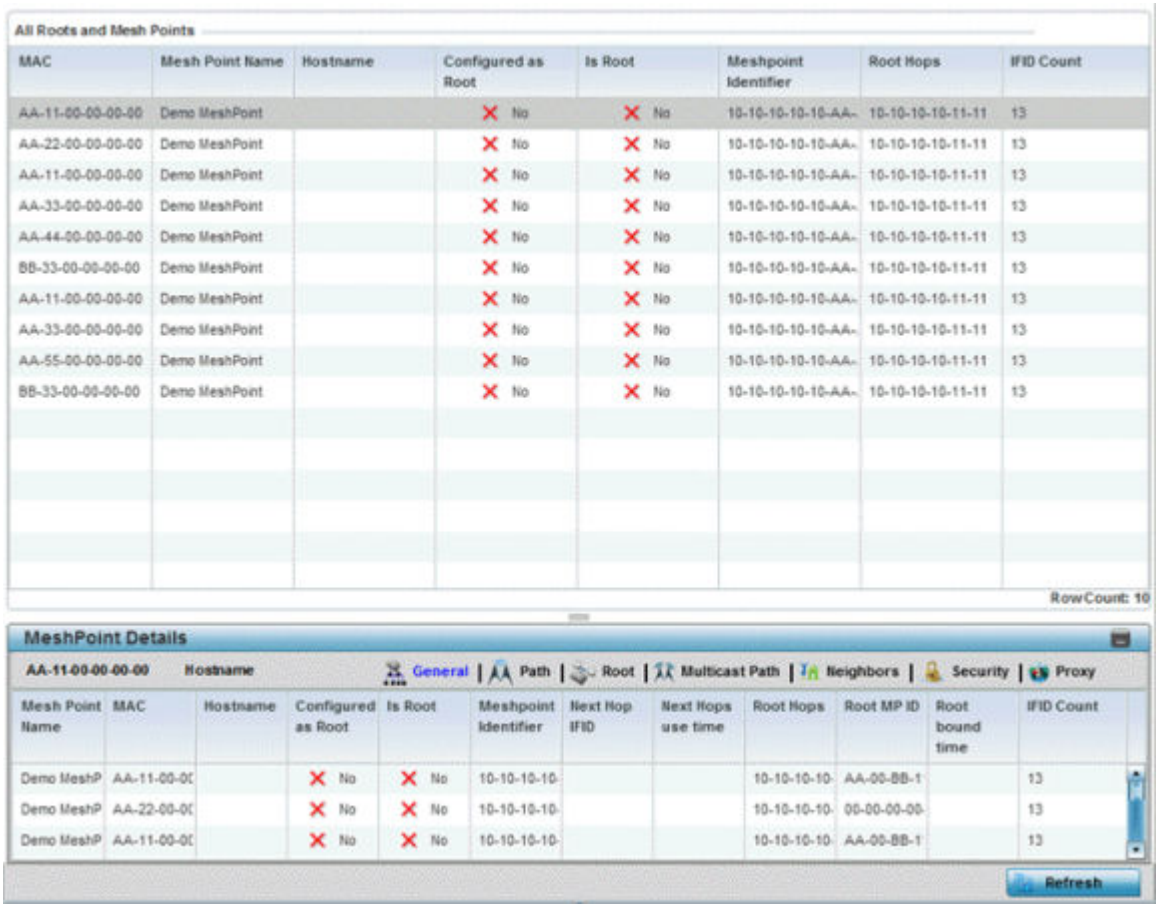
The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Mesh Point** from the RF Domain menu.

The MCX Geographical View screen displays by default.

5 Click **Device Brief Info** from the top of the screen.

The **Device Brief Info** screen displays.




The **Device Brief Info** has the following sections:

- All Roots and Mesh Points - The top pane
- MeshPoint Details - The bottom pane

6 Refer the following table for the All Roots and Mesh Points table information:

| | |
|---|---|
| MAC | Displays the MAC Address of each configured mesh point in the RF Domain. |
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Hostname | Displays the administrator assigned hostname for each configured mesh point in the RF Domain. |
| Configured as Root | A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (**Yes**/**No**). |
| Is Root | Indicates whether the current mesh point is a root mesh point (**Yes**/**No**). |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Root Hops | The number of devices between the selected mesh point and the destination device. |
| IFID Count | Displays the number of Interface IDs (IFIDs) associated with all the configured mesh points in the RF Domain. |

The Mesh Point Details field on the bottom portion of the screen displays the following tabs:

- General
- Path
- Root
- Multicast Path
- Neighbors
- Security
- Proxy

7 Refer the following table for the General tab table information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| MAC | Displays the MAC Address of each configured mesh point in the RF Domain. |
| Hostname | Displays the administrator assigned hostname for each configured mesh point in the RF Domain. |
| Configured as Root | A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (**Yes**/**No**). |
| Is Root | Indicates whether the current mesh point is a root mesh point (**Yes**/**No**). |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Interface ID | Uniquely identifies an interface associated with the ID. Each mesh point on a device can be associated with one or more interfaces. |
| Root Interface | Lists the radio interface on which the mesh point operates |
| Next Hop IFID | Identifies the ID of the interface on which the next hop for the mesh network can be found. |
| Next Hop Use Time | Lists the time when the next hop in the mesh network topology was last utilized. |
| Root Hops | Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out. |
| Root MP ID | Lists the interface ID of the interface on which the next hop for the mesh network can be found. |
| Root Bound Time | Displays the duration this mesh point has been connected to the mesh root. |
| IFID Count | Displays the number of IFIDs associated with all the configured mesh points in the RF Domain. |

8 Refer the following table for the Path tab table information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Destination | The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh. |
| Is Root | A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (**Yes**/**No**). |

| | |
|---|---|
| MiNT ID | Displays the MiNT Protocol ID for the global mint area identifier. This area identifier separates two overlapping mint networks and need only be configured if the administrator has two mint networks that share the same packet broadcast domain. |
| Next Hop IFID | The Interface ID of the mesh point that traffic is being directed to. |
| Hops | Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out. |
| Mobility | Displays whether the mesh point is a mobile or static node. Displays **`True`** when the device is mobile and **`False`** when the device is not mobile. |
| Metric | A measure of the quality of the path. A lower value indicates a better path. |
| State | Indicates whether the path is currently **`Valid`** of **`Invalid`**. |
| Binding | Indicates whether the path is **`bound`** or **`unbound`**. |
| Timeout | The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is **`Init`** or **`In Progress`**, the timeout duration has no significance. If the state is **`Enabled`**, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is **`Failed`**, the timeout duration is the amount of time after which the system will retry. |
| Sequence | The sequence number also known as the destination sequence number. It is updated whenever a mesh point receives new information about the sequence number from *RREQ*, *RREP*, or *RERR* messages that may be received related to that destination. |

9 Refer the following table for the Root tab table information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Recommended | Displays the root that is recommended by the mesh routing layer. |
| Root MPID | The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration. |
| Next Hop IFID | The IFID of the next hop. The IFID is the MAC Address on the destination device. |
| Radio Interface | This indicates the interface that is used by the device to communicate with this neighbor. The values are **`2.4`** and **`5.8`**, indicating the frequency of the radio that is used to communicate with the neighbor. |
| Bound | Indicates whether the root is bound or unbound. |
| Metric | Displays the computed path metric between the neighbor and their root mesh point. |
| Interface Bias | This field lists any bias applied because of the Preferred Root Interface Index. |
| Neighbor Bias | This field lists any bias applied because of the Preferred Root Next-Hop Neighbor IFID. |
| Root Bias | This field lists any bias applied because of the Preferred Root MPID. |

10 Refer the following table for the Multicast Path tab table information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Subscriber Name | Lists the subscriber name is used to distinguish between other mesh point neighbors both on the same device and on other devices. |
| Subscriber MPID | Lists the subscriber ID to distinguish between other mesh point neighbors both on the same device and on other devices. |

| | |
|---|---|
| Group Address | Displays the MAC address used for the Group in the mesh point. |
| Timeout | The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is **Init** or **In Progress**, the timeout duration has no significance. If the state is **Enabled**, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is **Failed**, the timeout duration is the amount of time after which the system will retry. |

11 Refer the following table for the Neighbors tab table information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Neighbor MP ID | The MAC Address that the device uses to define the mesh point in the device that the neighbor is a part of. It is used to distinguish the device that is the neighbor. |
| Neighbor IFID | The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh. |
| Root MP ID | The mesh point ID of the neighbor's root mesh point. |
| Is Root | A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. **Yes** if the mesh point that is the neighbor is a root mesh point or **No** if the Mesh Point that is the neighbor is not a root. |
| Mobility | Displays whether the mesh point is a mobile or static node. Displays **True** when the device is mobile and **False** when the device is not mobile. |
| Radio Interface | This indicates the interface that is used by the device to communicate with this neighbor. The values are **2.4** and **5.8**, indicating the frequency of the radio that is used to communicate with the neighbor. |
| Mesh Root Hops | The number of devices between the neighbor and its root mesh point. If the neighbor is a root mesh point, this value will be **0**. If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be **1**. Each mesh point between the neighbor and its root mesh point is counted as 1 hop. |
| Resourced | Displays whether the mesh point has been resourced or not. The Mesh Connex neighbor table can contain more neighbors than the AP supports. If the neighbor is resourced, it will take away a one of the resources for a wireless client device to be used for meshing. Displays **True** when the device is resourced and **False** when the device is not. |
| Link Quality | An abstract value depicting the quality of the mesh link between the device and the neighbor. The range is from 0 (weakest) to 100 (strongest). |
| Link Metric | This value shows the computed path metric from the device to the neighbor mesh point using this interface. The lower the number the better the possibility that the neighbor will be chosen as the path to the root mesh point. |
| Root Metric | The computed path metric between the neighbor and their root mesh point. |

| | |
|---|---|
| Rank | The rank is the level of importance and is used for automatic resource management.<br>• **8** – The current next hop to the recommended root.<br>• **7** – Any secondary next hop to the recommended root to has a good potential route metric.<br>• **6** – A next hop to an alternate root node.<br>• **5** – A downstream node currently hopping through to get to the root.<br>• **4** – A downstream node that could hop through to get to the root, but is currently not hopping through any node (look at authentication, as this might be an issue).<br>• **3** – A downstream node that is currently hopping through a different node to get to the root, but could potentially have a better route metric if it hopped through this node.<br>• **2** – Reserved for active peer to peer routes and is not currently used.<br>• **1** - A neighbor bound to the same recommended root but does not have a potential route metric as good as the neighbors ranked 8 and 7.<br>• **0** – A neighbor bound to a different root node.<br>• **-1** – Not a member of the mesh as it has a different mesh ID.<br>All client devices hold a rank of 3 and can replace any mesh devices lower than that rank. |
| Age | Displays the number of miliseconds since the mesh point last heard from this neighbor. |

12 Refer the following table for the Security tab table information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Radio Interface | This indicates the interface that is used by the device to communicate with this neighbor. The values are **2.4** and **5.8**, indicating the frequency of the radio that is used to communicate with the neighbor. |
| Interface ID | The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces. |
| State | Displays the Link State for each mesh point:<br>• **Init** - indicates the link has not been established or has expired.<br>• **Enabled –** indicates the link is available for communication.<br>• **Failed** - indicates the attempt to establish the link failed and cannot be retried yet.<br>• **In Progress –** indicates the link is being established but is not yet available. |
| Timeout | Displays the maximum value in seconds that the link is allowed to stay in the In Progress state before timing out. |
| Keep Alive | **Yes** indicates that the local MP will act as a supplicant to authenticate the link and not let it expire (if possible). **No** indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP. |

13 Refer the following table for the Proxy tab table information:

| | |
|---|---|
| Mesh Point Name | Displays the name of each configured mesh point in the RF Domain. |
| Destination Addr | The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID. |
| Proxy Address | Displays the MAC Address of the proxy used in the mesh point. |
| Age | Displays the age of the proxy connection for each of the mesh points in the RF Domain. |

| | |
|---|---|
| Proxy Owner | The owner (MPID) is used to distinguish the device that is the neighbor. |
| VLAN | The VLAN ID used as a virtual interface with this proxy. A value of 4095 indicates that there is no VLAN ID. |

14 Periodically click **Refresh** to update the status of the screen.

*Device Data Transmit*

To view mesh point statistics for RF Domain member APs and their connected clients:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

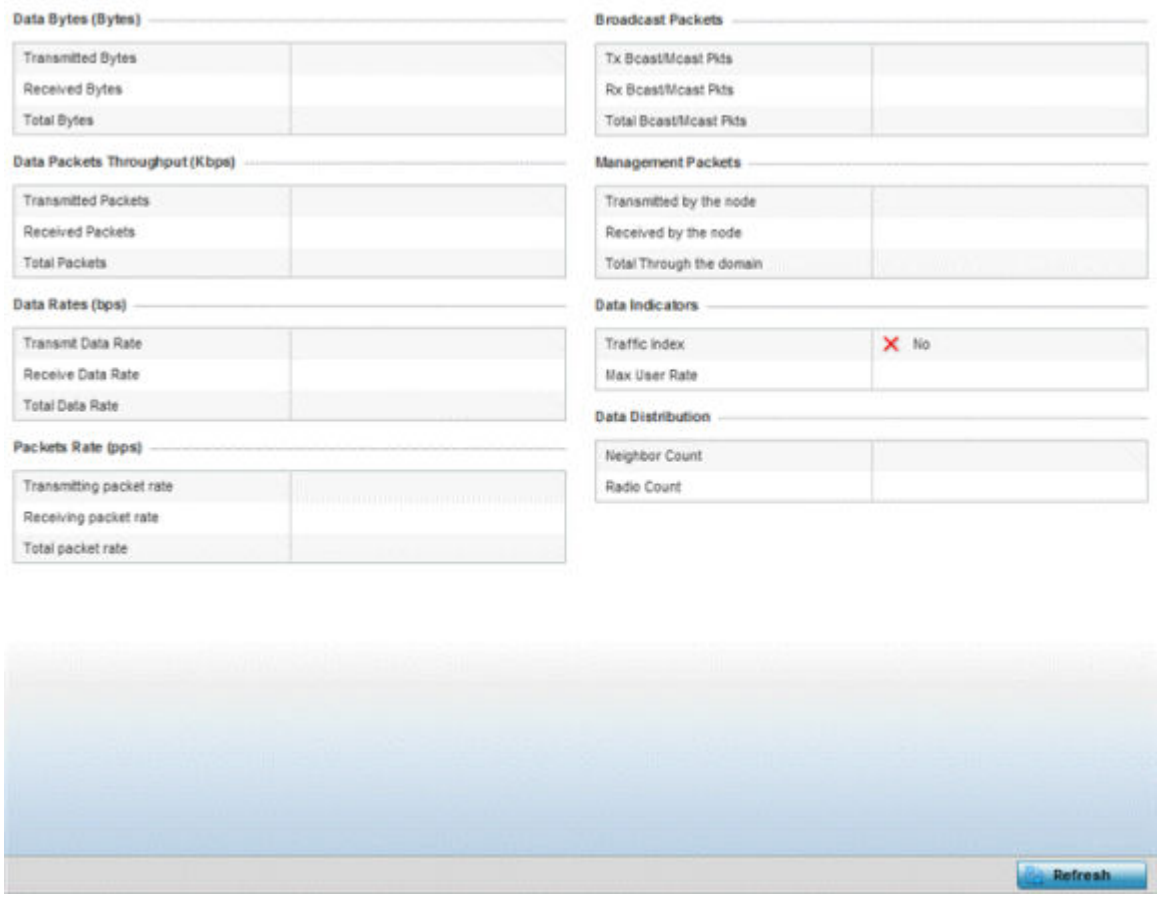
The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Mesh Point** from the RF Domain menu.

The MCX Geographical View screen displays by default.

5 Click **Device Data Transmit** from the top of the screen.

The **Device Data Transmit** screen displays.



6 Review the following transmit and receive statistics for Mesh nodes:

| | |
|---|---|
| Data Bytes (Bytes): Transmitted Bytes | Displays the total amount of data, in Bytes, transmitted by Mesh Points in the RF Domain. |
| Data Bytes (Bytes): Received Bytes | Displays the total amount of data, in Bytes, received by Mesh Points in the RF Domain. |
| Data Bytes (Bytes): Total Bytes | Displays the total amount of data, in Bytes, transmitted and received by Mesh Points in the RF Domain. |
| Data Packets Throughput (Kbps): Transmitted Packets | Displays the total amount of data, in packets, transmitted by Mesh Points in the RF Domain. |
| Data Packets Throughput (Kbps): Received Packets | Displays the total amount of data, in packets, received by Mesh Points in the RF Domain. |
| Data Packets Throughput (Kbps): Total Packets | Displays the total amount of data, in packets, transmitted and received by Mesh Points in the RF Domain. |
| Data Rates (bps): Transmit Data Rate | Displays the average data rate, in kbps, for all data transmitted by Mesh Points in the RF Domain. |
| Data Rates (bps): Receive Data Rate | Displays the average data rate, in kbps, for all data received by Mesh Points in the RF Domain. |
| Data Rates (bps): Total Data Rate | Displays the average data rate, in kbps, for all data transmitted and received by Mesh Points in the RF Domain. |
| Packets Rate (pps): Transmitting Packet rate | Displays the average packet rate, in packets per second, for all data transmitted and received by Mesh Points in the RF Domain. |
| Packets Rate (pps): Received Packet rate | Displays the average packet rate, in packets per second, for all data received and received by Mesh Points in the RF Domain. |
| Packets Rate (pps): Total Packet Rate | Displays the average data packet rate, in packets per second, for all data transmitted and received by Mesh Points in the RF Domain. |
| Data Packets Dropped and Errors: Tx Dropped | Displays the total number of transmissions that were dropped Mesh Points in the RF Domain. |
| Data Packets Dropped and Errors: Rx Errors | Displays the total number of receive errors from Mesh Points in the RF Domain. |
| Broadcast Packets: Tx Bcast/Mcast Pkts | Displays the total number of broadcast and multicast packets transmitted from Mesh Points in the RF Domain. |
| Broadcast Packets: Rx Bcast/Mcast Pkts | Displays the total number of broadcast and multicast packets received from Mesh Points in the RF Domain. |
| Broadcast Packets: Total Bcast/Mcast Pkts | Displays the total number of broadcast and multicast packets transmitted and received from Mesh Points in the RF Domain. |
| Management Packets: Transmitted by the node | Displays the total number of management packets that were transmitted through the Mesh Point node. |
| Management Packets: Received by the node | Displays the total number of management packets that were received through the Mesh Point node. |
| Management Packets: Total Through the domain | Displays the total number of management packets that were transmitted and received through the Mesh Point node. |
| Data Indicators: Traffic Index | Displays **`True`** of **`False`** to indicate whether or not a traffic index is present. |

| | |
|---|---|
| Data Indicators: Max User Rate | Displays the maximum user throughput rate for Mesh Points in the RF Domain. |
| Data Distribution: Neighbor Count | Displays the total number of neighbors known to the Mesh Points in the RF Domain. |
| Data Distribution: Neighbor Count | Displays the total number of neighbor radios known to the Mesh Points in the RF Domain. |

7 Select the Refresh button to update the screen's statistics counters to their latest values.

## SMART RF - Overview

When invoked by an administrator, Smart RF *(Self-Monitoring At Run Time)* instructs access point radios to change to a specific channel and begin beaconing using the maximum available transmit power. Within a well-planned deployment, any RF Domain member access point radio should be reachable by at least one other radio. Smart RF records signals received from its neighbors as well as signals from external, unmanaged radios. AP-to-AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

The **RF Domain > SMART RF** option has the following sub-menus:

- SMART RF - Summary on page 957.
- SMART RF - Details - Details on page 960.
- SMART RF - Details - Energy Graph on page 961.
- SMART RF - History on page 962.

### *SMART RF - Summary*

The Summary screen enables administrators to assess the efficiency of RF Domain member device channel distributions, sources of interference potentially requiring Smart RF adjustments, top performing RF Domain member device radios and the number of power, channel and coverage changes required as part of a Smart RF performance compensation activity.

To view the Smart RF summary for RF Domain member access point radios:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

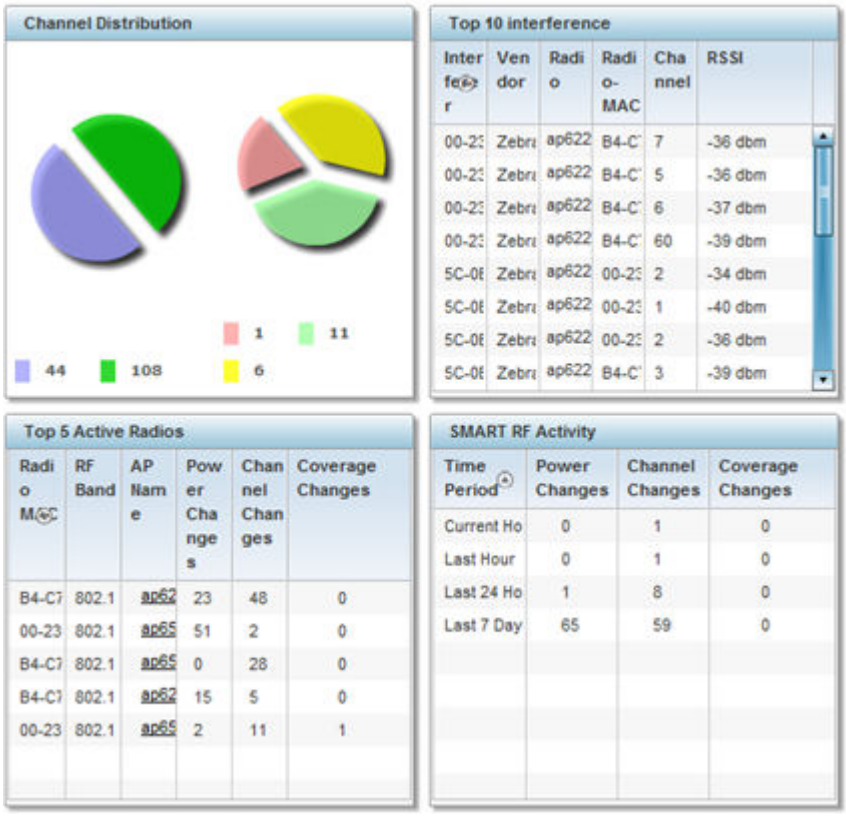
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **SMART RF** from the RF Domain menu.

The SMART RF Summary screen displays by default.




The Summary screen displays the following SMART RF related statistics:

5 Use the Channel Distribution area to determine how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. Use this data to assess whether the channel spectrum is being effectively utilized and whether channel changes are warranted to improve RF Domain member device performance.

6 Review the Top 10 interference table to assess RF Domain member devices whose level of interference exceeds the threshold set (from -100 to -10 dBm) for acceptable performance.

| | |
|---|---|
| Interferer | Lists the administrator defined name of the interfering RF Domain member device. |
| Vendor | Displays the vendor name (manufacturer) of the interfering RF Domain member device radio. |
| Radio MAC | Displays the factory encoded hardware MAC address assigned to the RF Domain member device radio. |
| Channel | Displays the channel each of the 10 poorly performing RF Domain member devices was detected on. Numerous interfering devices on the same channel could define the need for better channel segregation to reduce the levels of detected interference. |
| RSSI | Lists a RSSI *(received signal strength indication)* in dBm for those RF Domain member devices falling into the poorest performing 10 devices based on the administrator defined threshold value. |

7 Review the Top 5 Active Radios to assess the significance of any Smart RF initiated compensations versus their reported top performance.

| | |
|---|---|
| Radio MAC | Lists the hardware-encoded MAC address of each listed top performing RF Domain member device radio. |
| RF Band | Displays the top performing radio's operation band. This may help administrate whether more changes were required in the 2.4 GHz band then 5 GHz or vice versa. |
| AP Name | Lists the administrator-assigned AP name used to differentiate from other RF Domain member AP radios. The name displays in the form of a link that you can select to vie device information in greater detail. |
| Power Changes | Displays the number of Smart RF initiated power level changes reported for this top performing RF Domain member radio. |
| Channel Changes | Displays the number of Smart RF initiated channel changes reported for this top performing RF Domain member radio. |
| Coverage Changes | Displays the number of Smart RF initiated coverage changes reported for this top performing RF Domain member radio. |

8 Refer to the SMART RF Activity table to view the trending of Smart RF compensations.

| | |
|---|---|
| Time Period | Lists the frequency Smart RF activity is trended for the RF Domain. Trending periods include the **`Current Hour`**, **`Last 24 Hours`** or the **`Last Seven Days`**. Comparing Smart RF adjustments versus the last seven days enables an administrator to assess whether periods of interference and poor performance were relegated to just specific periods. |
| Power Changes | Displays the number of Smart RF initiated power level changes needed for RF Domain member devices during each of the three trending periods. Determine whether power compensations were relegated to known device outages or if compensations were consistent over the course of a day or week. |
| Channel Changes | Lists the number of Smart RF initiated channel changes needed for RF Domain member devices during each of the three trending periods. Determine if channel adjustments were relegated to known device count increases or decreases over the course of a day or week. |
| Coverage Changes | Displays the number of Smart RF initiated coverage changes needed for RF Domain member devices during each of the three trending periods. Determine if coverage changes were relegated to known device failures or known periods of interference over the course of a day or week. |

9 Click **Refresh** to update the Summary to its latest RF Domain Smart RF information.

### *SMART RF - Select Shutdown*

The Select Shutdown screen displays 2.4 GHz APs shutdown to maintain CCI *(co-channel interference)* levels within specified limits.

Note
This information is displayed only if select-shutdown is enabled in the smart-rf policy context. For more information, see select-shutdown.

1 Refer to the following table for the Smart RF → Select Shutdown related statistical data:

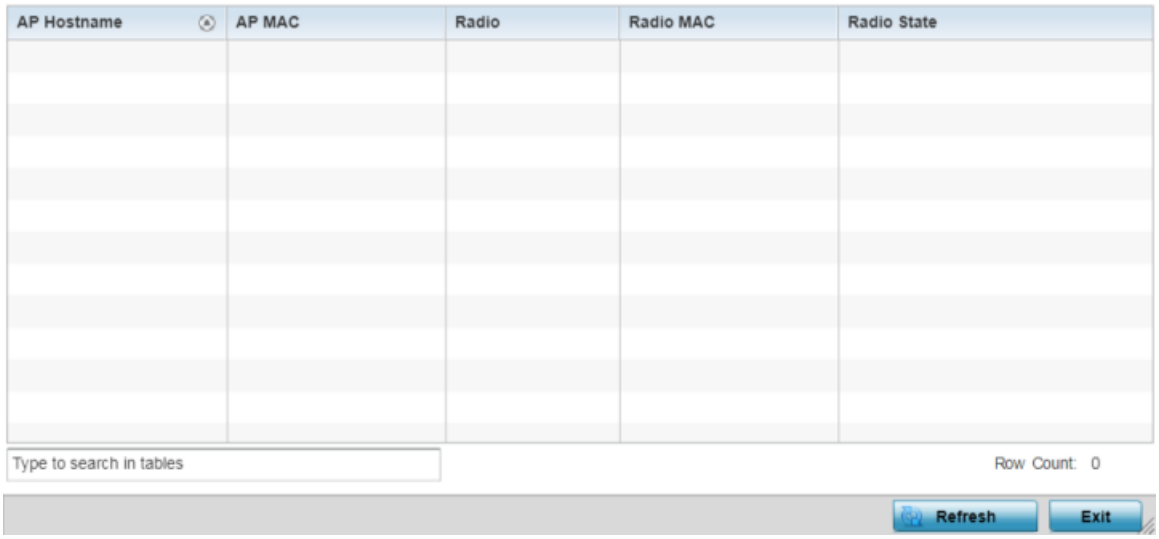



**Figure 429: RF-Domain → Smart RF → Select Shutdown**

2 Review the following configuration details:

| | |
|---|---|
| AP Hostname | Displays hostname of AP that was shutdown by Smart RF as part of the select shutdown feature.<br>The Smart RF select-shutdown option, auto-shutdowns selected 2.4 GHz radios, in dual-band networks, to maintain CCI levels within specified limits.<br><br>Note: For information on enabling select shutdown, see Configuring Smart RF Select Shutdown Settings on page 644. |
| AP MAC | Displays the AP's MAC address |
| Radio | Displays the radio that was shutdown |
| Radio MAC | Displays the Radio's MAC address |
| Radio Status | Displays the Radio's current status |

3 Click **Refresh** to update the Select Shutdown screen with the RF Domain Smart RF information.

*SMART RF - Details - Details*

To view Smart RF stats for RF Domain member AP radios:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

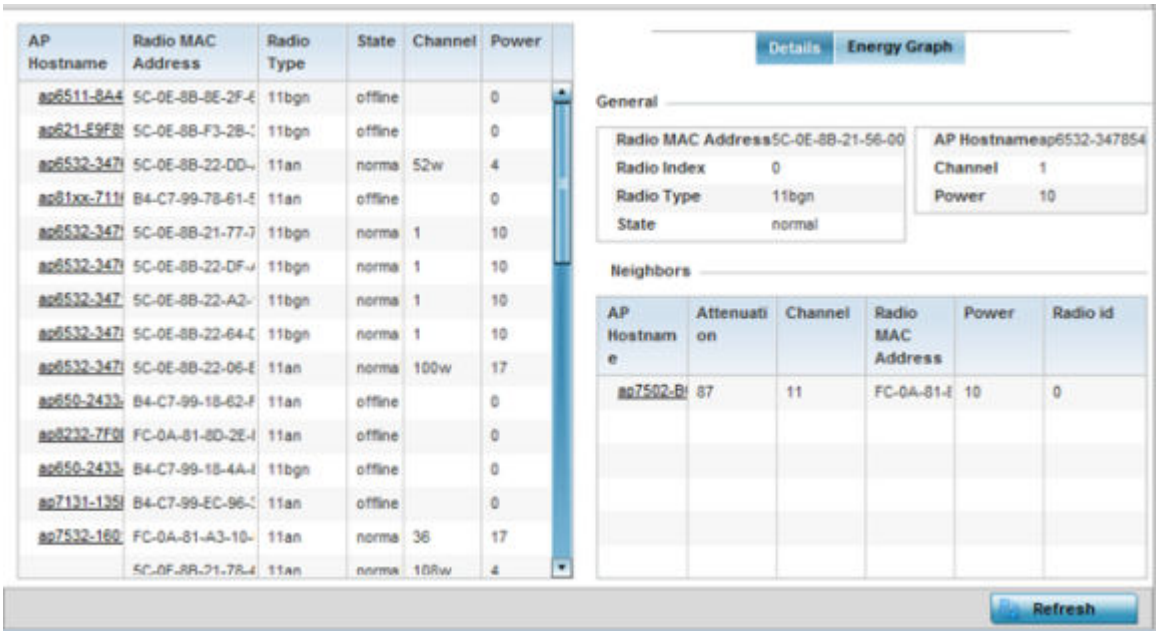
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand **SMART RF** from the RF Domain menu.
5 Click **Details**.

The **SMART RF Details** screen displays.




6 Refer to the General field to review and assess the radio's:

- factory-encoded hardware MAC address.
- administrator-assigned index.
- 802.11 radio type.
- current operational state.
- AP's administrator-assigned hostname.
- current operating channel and power.

7 Refer to the Neighbors table to review the attributes of neighbor radio resources available for Smart RF radio compensations for other RF Domain member device radios. Select individual AP hostnames to review RF Domain member radios in greater detail.

Note

*Attenuation* is a measure of the reduction of signal strength during transmission. Attenuation is the opposite of amplification, and is normal when a signal is sent from one point to another. If the signal attenuates too much, it becomes unintelligible. Attenuation is measured in decibels.

The radio's current operating channel is also displayed, as is the radio's hard coded MAC address transmit power level and administrator assigned ID.

8 Select **Refresh** to update the screen to its latest values.

### *SMART RF - Details - Energy Graph*

The SMART RF Energy Graph screen displays the RF Domain member AP's radio's operating channel, noise level and neighbor count. Use this information to assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios.

To access the SMART RF Energy Graph screen:

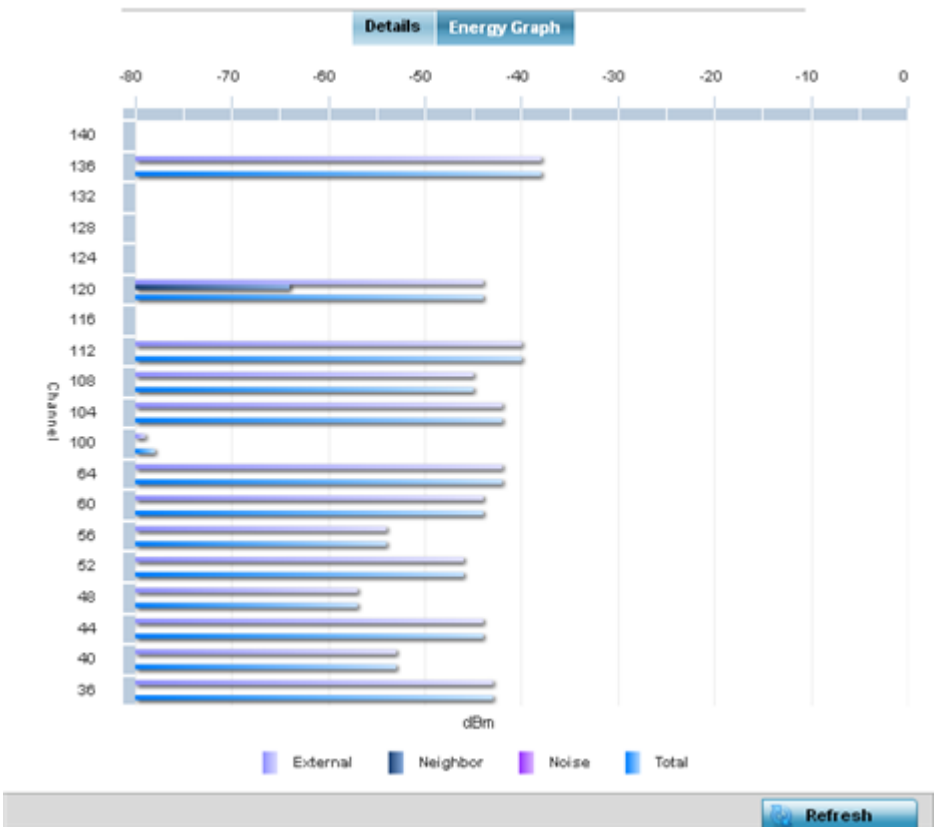
1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand **SMART RF** from the RF Domain menu.
5 Click **Details**.
6 Select the **Energy Graph** tab.




7 Select **Refresh** to update the screen to its latest values.

*SMART RF - History*

Select Smart RF History to review Smart RF events impacting RF Domain member devices.

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

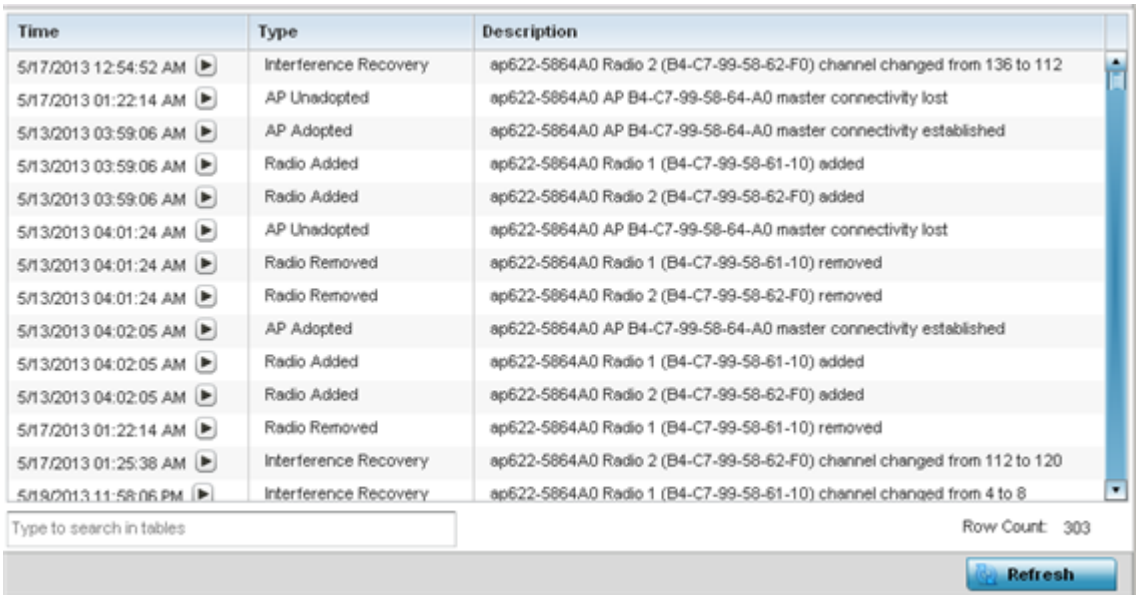
The **System** node expands to display the RF Domains created within the managed network.

3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand **SMART RF** from the RF Domain menu.

5 Click the **SMART RF History** tab.




The SMART RF History screen displays the following RF Domain member historical data:

| | |
|---|---|
| Time | Displays the time stamp when Smart RF status was updated on behalf of a Smart RF adjustment within the selected RF Domain. |
| Type | Lists a high-level description of the Smart RF activity initiated for a RF Domain member device. |
| Description | Provides a more detailed description of the Smart RF event in respect to the actual Smart RF calibration or adjustment made to compensate for detected coverage holes and interference. |

6 Select **Refresh** to update the screen to its latest values.

## WIPS

WIPS *(Wireless Intrusion Protection System)* provides continuous protection against wireless threats and acts as an additional layer of security complementing wireless VPNs and traditional encryption and authentication schemes. WIPS utilizes dedicated sensor devices designed to actively detect and locate unauthorized access points within a controller or service platform managed RF Domain.

Refer to the WIPS screens to review a client blacklist and rogue device detection events reported by RF Domain member APs.

For more information, see:

- WIPS Client Blacklist
- WIPS Events

### *WIPS Client Blacklist*

The **Client Blacklist** screen displays clients detected by WIPS and removed from RF Domain. Blacklisted clients are not allowed to associate to RF Domain member AP radios.

To view the WIPS client blacklist:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

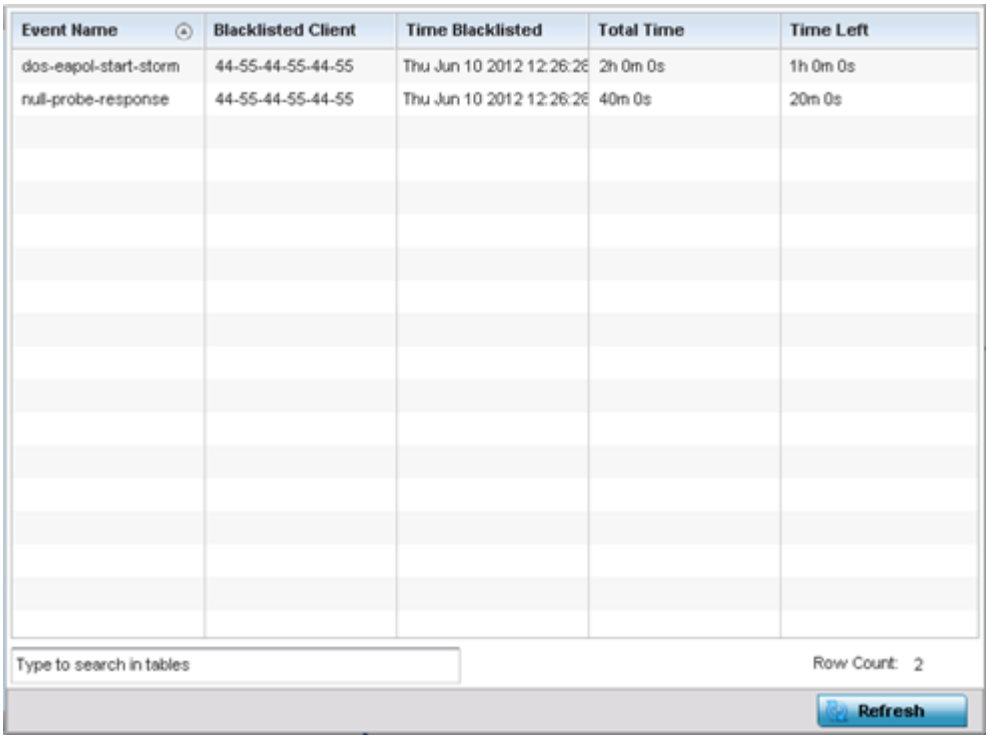
The **System** node expands to display the RF Domains created within the managed network.

3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand **WIPS** from the RF Domain menu.

The **WIPS Client Blacklist** screen displays by default.




5 Review the WIPS **Client Blacklist** screen information:

| | |
|---|---|
| Event Name | Displays the name of the blacklisting wireless intrusion event detected by a RF Domain member AP. |
| Blacklisted Client | Displays the MAC address (hardware identifier) of the unauthorized (blacklisted) client intruding the RF Domain. |
| Time Blacklisted | Displays the time when the wireless client was blacklisted by a RF Domain member AP. |
| Total Time | Displays the duration the unauthorized (now blacklisted) device remained in the RF Domain. This is the duration for which the network was potentially vulnerable to the unauthorized device. |
| Time Left | Displays the time the blacklisted client remains on the list. |

6 Select **Refresh** to update the screen to its latest values.

*WIPS Events*

Refer to the WIPS Events screen to assess WIPS events detected by RF Domain member access point radios and reported to the controller or service platform.

To view the rogue access point statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

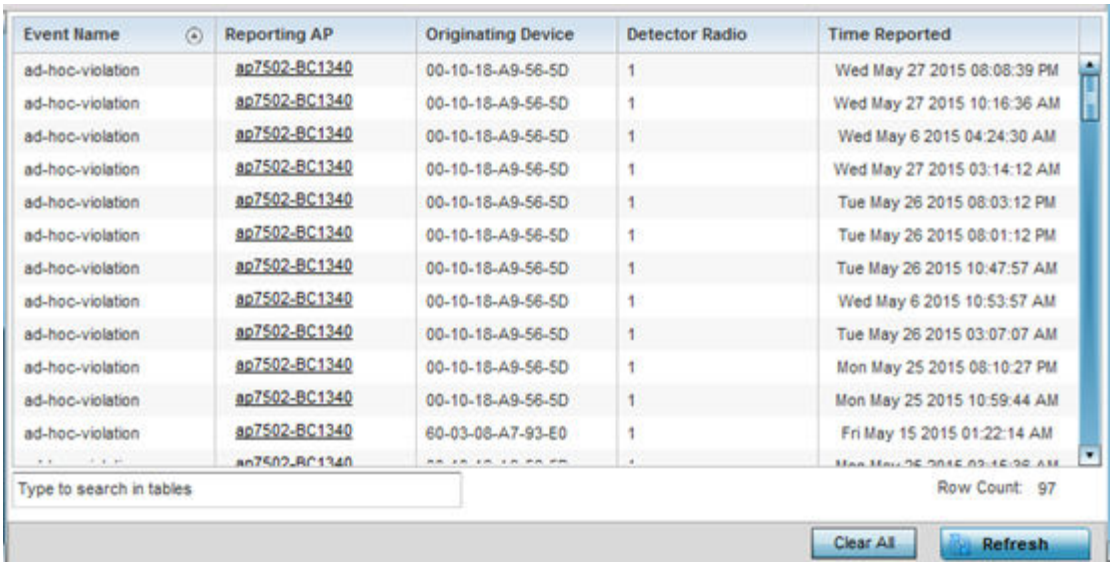
The **System** node expands to display the RF Domains created within the managed network.

3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand **WIPS** from the RF Domain menu.
5 Click **WIPS Event**.

The WIPS Event screen displays.




6 Review the WIPS Events screen information:

| | |
|---|---|
| Event Name | Displays the event name of the intrusion detected by a RF Domain member AP radio. |
| Reporting AP | Displays the MAC address (hardware identifier) of the RF Domain member AP reporting the event. |
| Originating Device | Displays the MAC address of the device generating the event. |
| Detector Radio | Displays the index number of the AP's radio detecting the event. |
| Time Reported | Displays a time stamp of when the event was reported by the RF Domain member AP radio. |

7 Select **Clear All** to clear the statistics counters and begin a new data collection.
8 Select **Refresh** to update the screen to its latest values.

## Captive Portal

A *captive portal* is an access policy for providing temporary and restrictive access to the controller or service platform managed wireless network. Captive portal authentication is used primarily for guest or visitor access to the network, but is increasingly being used to provide authenticated access to private network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static *WEP*, *WPA-PSK* or *WPA2-PSK* encryption.

To view the captive portal statistics for RF Domain member devices:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

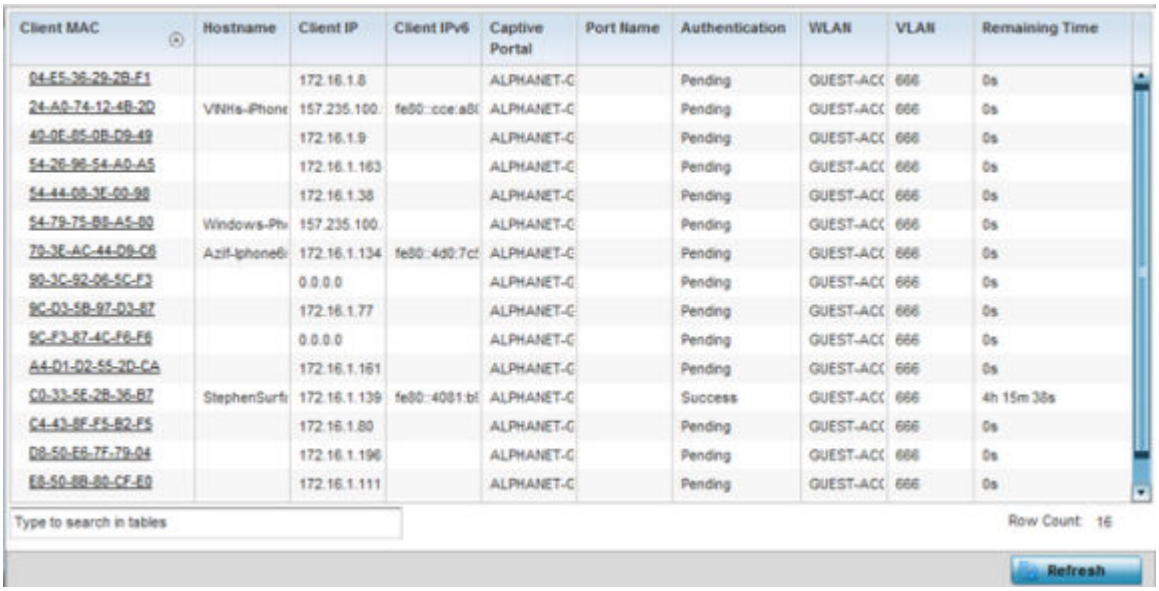
The **System** node expands to display the RF Domains created within the managed network.

3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Captive Portal** from the RF Domain menu.

The Captive Portal screen displays.




5 Refer the table below for Captive Portal related statistical data:

| | |
|---|---|
| Client MAC | Displays the MAC address of each listed client requesting captive portal access to the controller, service platform or AP managed network. This address can be selected to display client information in greater detail. |
| Host Name | Displays the administrator-assigned hostname of the device requesting captive portal access to the network's RF Domain resources. |
| Client IP | Displays the IPv4 formatted address of each listed client using its connected RF Domain member AP for captive portal access. |

| | |
|---|---|
| Client IPv6 | Displays any IPv6 formatted address of any listed client using its connected RF Domain member AP for captive portal access. IPv6 is the latest revision of the IP *(Internet Protocol)* designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Captive Portal | Lists the name of the RF Domain captive portal currently being utilized by each listed client. |
| Port Name | Lists the name virtual port used for captive portal session direction. |
| Authentication | Displays the authentication status of requesting clients attempting to connect to the controller, service platform or AP via the captive portal. |
| WLAN | Displays the name of the WLAN the requesting client would use for interoperation with the controller, service platform or AP. |
| VLAN | Displays the name of the VLAN the client would use as a virtual interface for captive portal operation with the controller, service platform or AP. |
| Remaining Time | Displays the time after which a connected client is disconnected from the captive portal. |

6 Select **Refresh** to update the screen to its latest values.

## Application Visibility

RF Domain member devices inspect every byte of each application header packet allowed to pass through the WiNG managed network. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. For information on categorizing, filtering and logging the application data allowed to proliferate the WiNG managed network, refer to Application on page 718 and Application Group on page 720.

Note
The WiNG 7.1 release does not support DPI on AP505 and AP10 model access points. This feature will be supported in future releases.

To view the application utilization statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

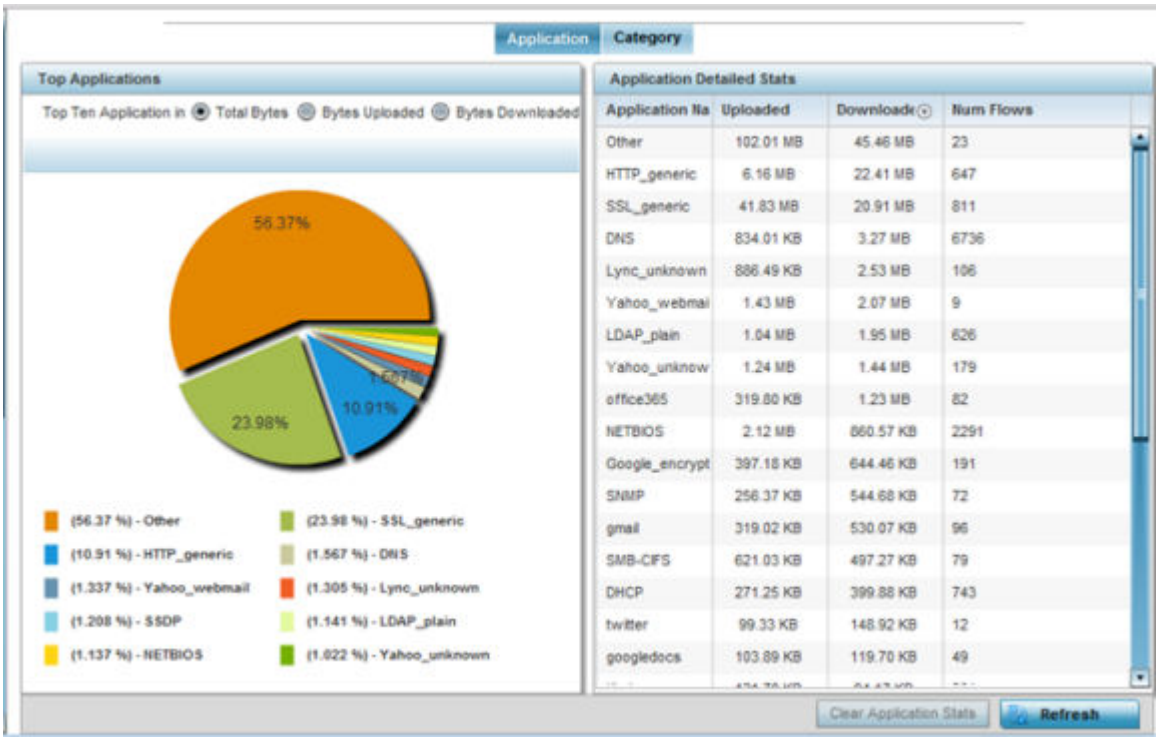
The **System** node expands to display the RF Domains created within the managed network.

3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **Application Visibility** from the RF Domain menu.

The **Application Visibility > Application** screen displays.




5 Refer to the Top Applications graph to assess the most prolific, and allowed, application data passing through RF Domain member devices.

| | |
|---|---|
| Total Bytes | Displays the top ten RF Domain member utilized applications in respect to total data bytes passing through the RF Domain member WiNG managed network. These are only the administrator allowed applications approved for proliferation within the RF Domain member device. |
| Bytes Uploaded | Displays the top ten RF Domain member applications in respect to total data bytes uploaded through the RF Domain member WiNG managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority). |
| Bytes Downloaded | Displays the top ten RF Domain member applications in respect to total data bytes downloaded from the RF Domain member WiNG managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority). |

6 Refer to the Application Detailed Stats table to assess specific application data utilization:

| | |
|---|---|
| Application Name | Lists the RF Domain member allowed application name whose data (bytes) are passing through the WiNG managed network. |
| Uploaded | Displays the number of uploaded application data (in bytes) passing the through the WiNG managed network. |
| Downloaded | Displays the number of downloaded application data (in bytes) passing the through the WiNG managed network. |

| | |
|---|---|
| Num Flows | Lists the total number of application data flows passing through RF Domain member devices for each listed application. An application flow can consist of packets in a specific connection or media stream. Application packets with the same source address/port and destination address/port are considered one flow. |

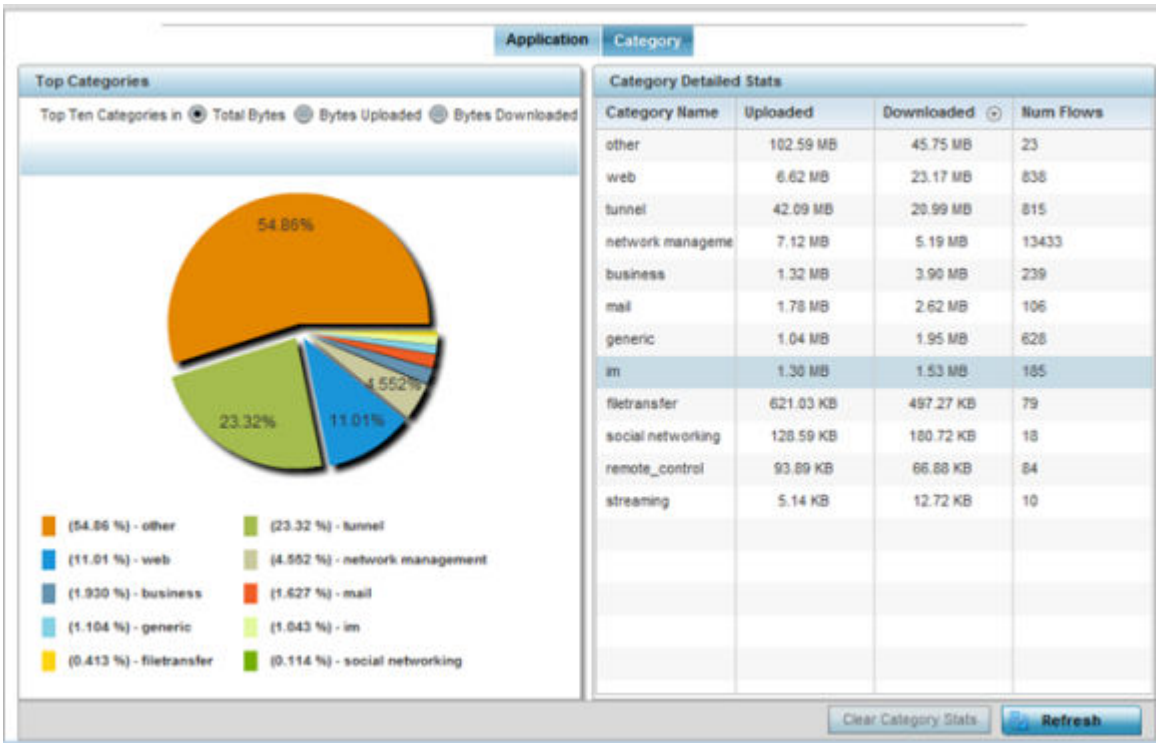
7 Click **Clear Application Stats** to clear the application assessment data counters and begin a new assessment.

8 Periodically, click **Refresh** to update the statistics counters to their latest values.

9 Select the **Category** tab.

Categories are existing WiNG or user defined application groups (video, streaming, mobile, audio etc.) that assist administrators in filtering (allowing or denying) application data. For information on categorizing application data, refer to Application on page 718 and Application Group on page 720.

The **Application Visibility > Category** screen displays.




Refer to the Top Categories graph to assess the most prolific, and allowed, application data categories utilized by RF Domain member devices.

| | |
|---|---|
| Total Bytes | Displays the top ten RF Domain member application categories in respect to total data bytes passing through the RF Domain member WiNG managed network. These are only the administrator allowed application categories approved for proliferation within the RF Domain. |
| Bytes Uploaded | Displays the top ten RF Domain member application categories in respect to total data bytes uploaded through the RF Domain member WiNG managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority). |

| | |
|---|---|
| Bytes Downloaded | Displays the top ten RF Domain member application categories in respect to total data bytes downloaded from the RF Domain member WiNG managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories and categories or adjusting their precedence (priority). |

Refer to the Category Detailed Stats table to assess specific application category data utilization:

| | |
|---|---|
| Category Name | Lists the RF Domain member allowed category whose application data (in bytes) is passing through the WiNG managed network. |
| Uploaded | Displays the number of uploaded application category data (in bytes) passing the through the WiNG managed network. |
| Downloaded | Displays the number of downloaded application category data (in bytes) passing the through the WiNG managed network. |
| Num Flows | Lists the total number of application category data flows passing through RF Domain member devices. A category flow can consist of packets in a specific connection or media stream. Packets with the same source address/port and destination address/port are considered one flow. |

10 Click **Clear Category Stats** to clear the application category assessment data counters and begin a new assessment.

11 Periodically, click **Refresh** to update the statistics counters to their latest values.

## Coverage Hole Detection

Refer to the **Statistics > RF Domain > WIPS** screens to review a client blacklist and events reported by a RF Domain member access point.

Refer to the Coverage Hole Detection screens to review any coverage hole adjustments reported by access points in the selected RF-Domain. When coverage hole recovery is enabled and a deployment area radio coverage hole is detected, Smart RF determines the radio's power increase compensation required based on a reporting client's SNR ratio. If a client's SNR is above the administrator threshold, its connected access point's transmit power is increased until the noise rate falls below the threshold.

### *Coverage Hole Summary*

To view a RF Domain's coverage hole summary:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

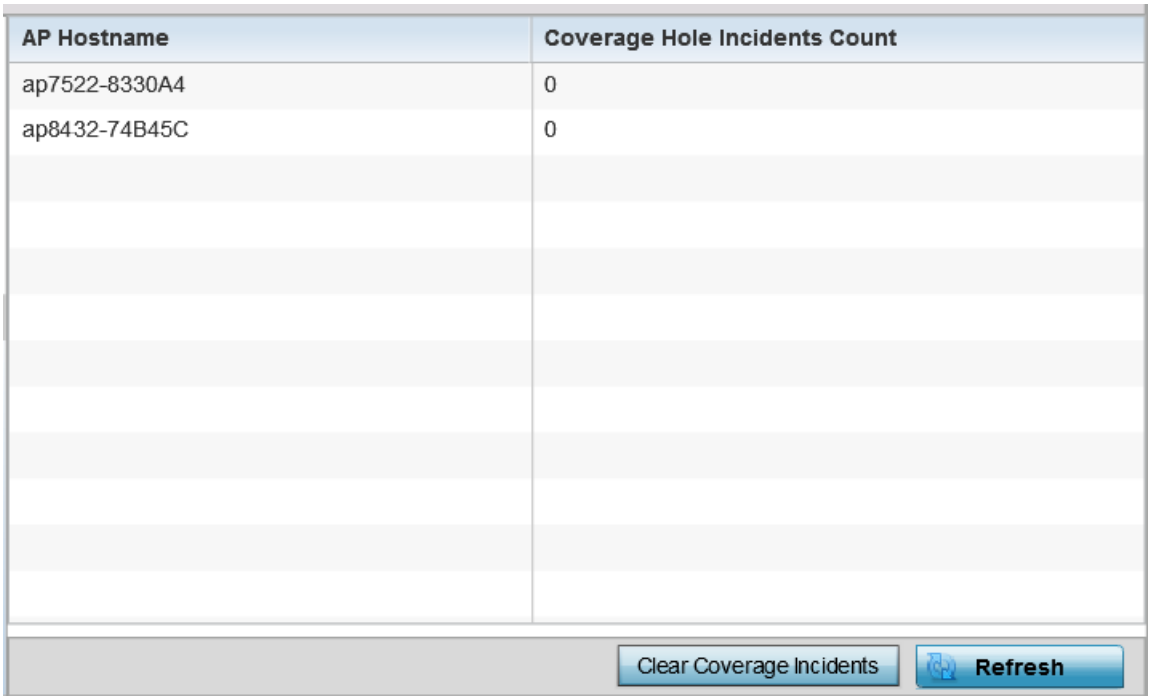
The **System** node expands to display the RF Domains created within the managed network.

3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand **Coverage Hole Detection** from the RF Domain menu.

The **Coverage Hole Detection > Summary** screen displays by default.




5 Refer the following table for the RF Domain coverage hole cumulative data:

| | |
|---|---|
| AP Hostname | Displays each RF Domain member access point hostname reporting a coverage hole compensation event. This can be helpful in assessing whether specific access points consistently report coverage holes and whether additional access point placements are required to compensate for poorly performing radios. |
| Coverage Hole Incidents Count | Lists each reporting access point's coverage hole incident count since the screen was last cleared. Periodically assess whether a specific access point's high incident count over a trended repeatable period warrants additional access point placements in that same radio coverage area to reduce a coverage hole. |

6 Click **Clear Coverage Incidents** to clear the statistics counters and begin a new coverage hole summary for RF Domain member access point radios.

7 Click **Refresh** to update the statistics counters to their latest values.

### *Coverage Hole Detail*

In addition to the RF Domain's *Coverage Hole Summary*, a specific access point's coverage hole history can be reviewed in detail. Consider using different RF Domain member access points or their connected clients to help validate the data reported before compensating for the coverage hole by increasing the radio transmit power of neighboring access points.

To view a RF Domain's member access point's coverage hole details:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

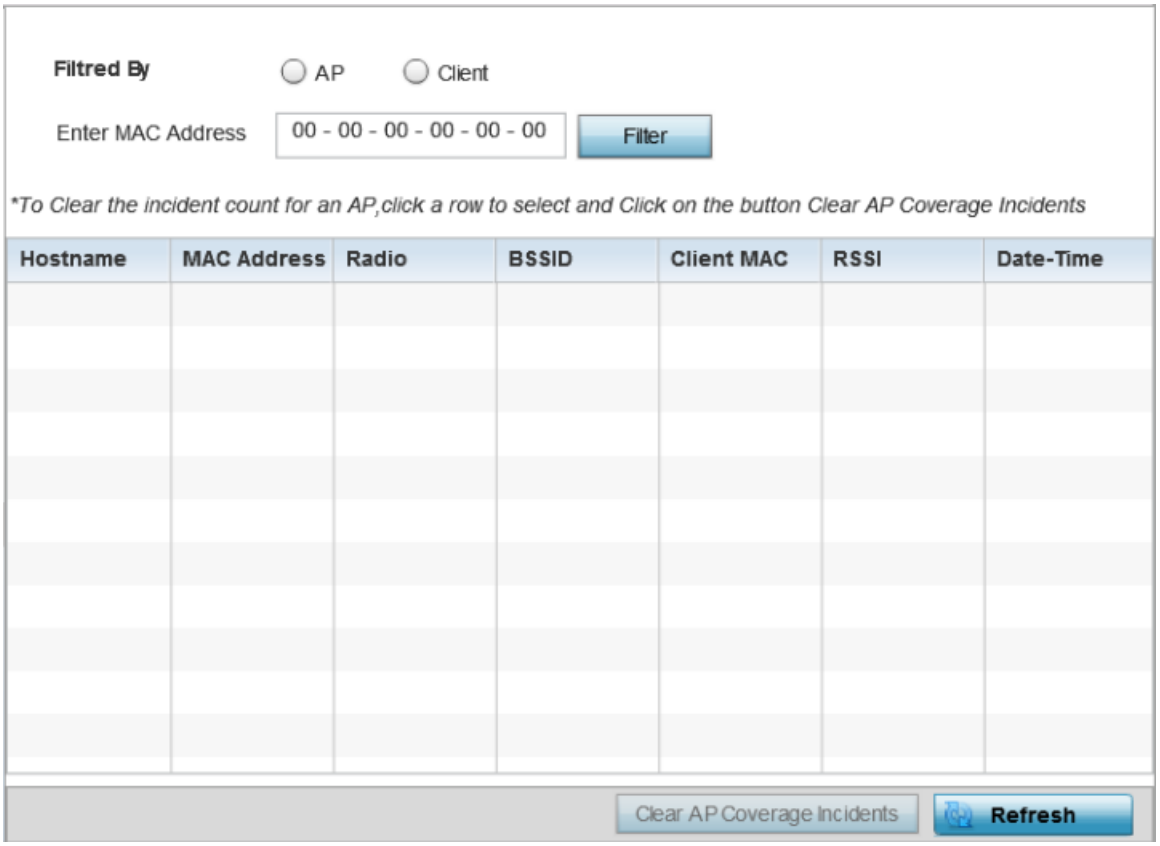
3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand **Coverage Hole Detection** from the RF Domain menu.

5 Select **Detail**.

The **Coverage Hole Detection > Detail** screen displays.




6 Use the **Filtered By** option to define whether the RF Domain's coverage hole details are provided by a selected access point or by a specific RF Domain member access point's connected *Client*. Consider filtering by different RF Domain member devices to validate the accuracy of a reported coverage hole before increasing the transmit power of neighboring radios to compensate.

7 Based on the **Filtered By** option selected in the previous step, in the **Enter MAC Address** field, enter the access point's MAC address or Hostname, or the client's MAC address.

This is the selected device reporting coverage hole details to the listed RF Domain member access point.

8 Select **Filter** to begin the coverage hole data collection using the access point or client details provided. Refer to the following to review the data reported:

| | |
|---|---|
| Hostname | Lists the administrator assigned hostname used as each listed access point's network identifier. This is the access point whose client(s) are reporting coverage hole RSSI data. |
| MAC address | Lists the reporting access point's MAC address. |
| Radio | Lists the access point radio receiving and reporting coverage hole RSSI data from the listed client MAC. |

| | |
|---|---|
| BSSID | Displays the BSSID *(basic service set identifier)* included in an access point's wireless packet transmissions. Packets need to go to their correct destination. While a SSID keeps packets within the correct WLAN there is usually multiple access points within each WLAN. A BSSID identifies the correct access point and its connected clients. |
| Client MAC | Lists each connected client's hardware encoded MAC address. This is the client reporting coverage hole RSSI data to its connected access point radio. |
| RSSI | Displays the RSSI *(Received Signal Strength Indicator)* of the detecting Access Radio or client. |
| Date-Time | Displays the date and time when each listed access point received its coverage hole indecent information. |

9 Click **Clear AP Coverage Incidents** to clear the statistics counters and begin a new coverage hole summary for RF Domain member access point radios.

10 Click **Refresh** to update the statistics counters to their latest values.

## Access Point Statistics

Access Point statistics screens displays access point *performance, health, version, client support, radio, mesh, interface, DHCP, firewall, WIPS, sensor, captive portal, NTP* and *load* information.

Access point statistics are reported from AP 6511, AP 6521, AP 6532, AP 6522, AP 6562, AP7131, AP 7161, AP 7181 or AP 8132 model access points in either Standalone or Controller AP mode orAP621 or AP650 model access points in *Dependent* mode. Dependent mode access points are reliant on their managing controller for their configuration file management and are unable to provide autonomous operation.

Access point statistics consists of the following:

- Health
- Device
- AP Upgrade
- Adoption
- AP Detection
- Wireless Clients
- Wireless LANs
- Policy Based Routing
- Radios
- Mesh
- Interfaces
- RTLS
- PPPoE
- OSPF
- L2TPv3
- VRRP
- Critical Resources
- Network
- DHCP Server

- Firewall
- VPN
- Certificates
- WIPS
- Sensor Servers
- Captive Portal
- Network Time
- Load Balancing
- Environmental Sensor

## AP Health

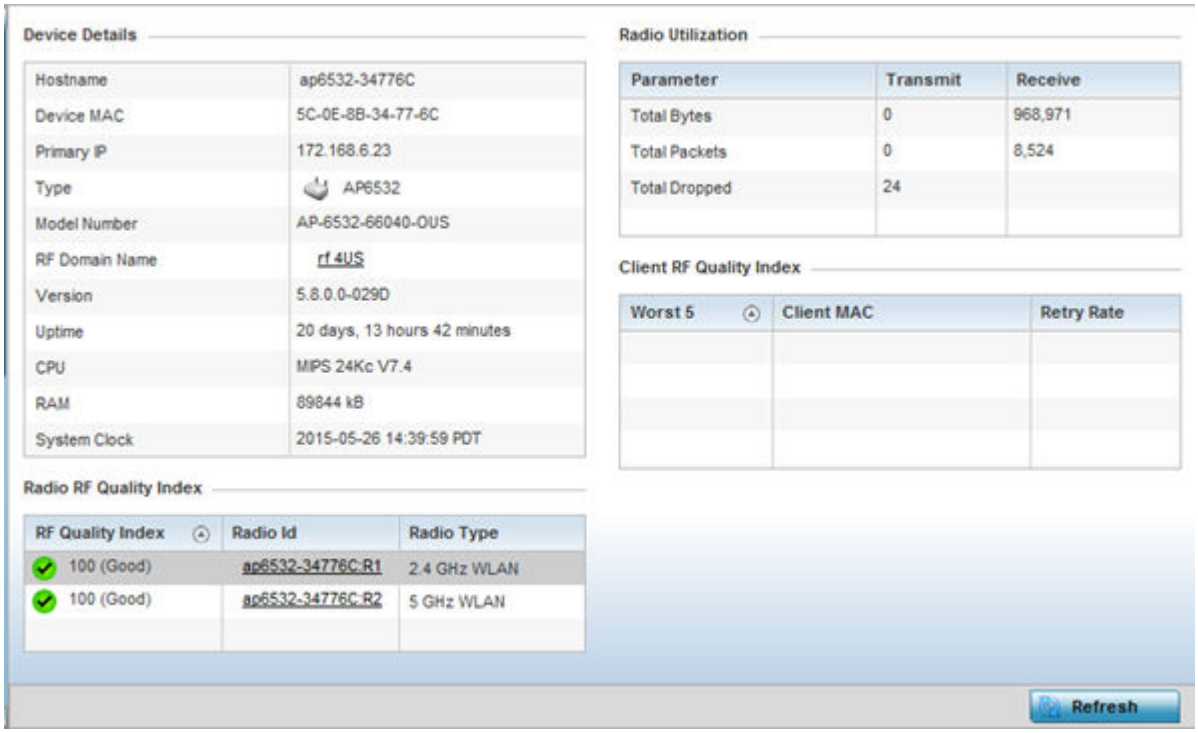
The **Health** screen displays a selected access point's hardware and software version. Use this information to refine the performance of an access point. The Health screen should also be the starting point for troubleshooting an access point, since it displays a high level overview of access point performance efficiency and client support capability.

To view an access point's health:

1 Select the **Statistics** tab from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.
4 Select **Health** from the left-hand side of the UI.




Review the different fields displayed on the **AP > Health** screen.

The **Device Details** field displays the following:

| | |
|---|---|
| **Hostname** | Displays the AP's unique name as assigned within the controller or service platform managed network. A hostname is assigned to a device connected to a computer network. |
| **Device MAC** | Displays the MAC address of the AP. This is factory assigned and cannot be changed. |
| **Primary IP** | Displays the IP address of assigned to this device either through DHCP or through static IP assignment. |
| **Type** | Displays the access point's model type. |
| **RF Domain Name** | Displays the access point's RF Domain membership. Unlike a controller or service platform, an access point can only belong to one RF Domain based on its model. The domain name appears as a link that can be selected to show RF Domain utilization in greater detail. |
| **Model Number** | Displays the access point's model number to help further differentiate the access point from others of the same model series and defined country of operation. |
| **Version** | Displays the access point's current firmware version. Use this information to assess whether an upgrade is required for better compatibility. |
| **Uptime** | Displays the cumulative time since the access point was last rebooted or lost power. |
| **CPU** | Displays the processor core. |
| **RAM** | Displays the free memory available with the RAM. |
| **System Clock** | Displays the system clock information. |

The **Radio RF Quality Index** field the following:

| | |
|---|---|
| **RF Quality Index** | Displays access point radios and their quality indices. RF quality index indicates the overall RF performance. The RF quality indices are:<br>• 0 – 50 (poor)<br>• 50 – 75 (medium)<br>• 75 – 100 (good) |
| **Radio id** | Displays a radio's hardware encoded MAC address The ID appears as a link that can be selected to show radio utilization in greater detail. |
| **Radio Type** | Identifies whether the radio is a 2.4 or 5 GHz. |

The **Radio Utilization** field displays the following:

| | |
|---|---|
| **Total Bytes** | Displays the total bytes of data transmitted and received by the access point since the screen was last refreshed. |
| **Total Packets** | Lists the total number of data packets transmitted and received by the access point since the screen was last refreshed. |
| **Total Dropped** | List the number of dropped data packets by an access point radio since the screen was last refreshed. |

The **Client RF Quality Index** field displays the following:

| | |
|---|---|
| Worst 5 | Displays clients having lowest RF quality within the network. |
| Client MAC | Displays the MAC addresses of the clients with the lowest RF indices. |
| Retry Rate | Displays the average number of retries per packet. A high number indicates possible network or hardware problems. |

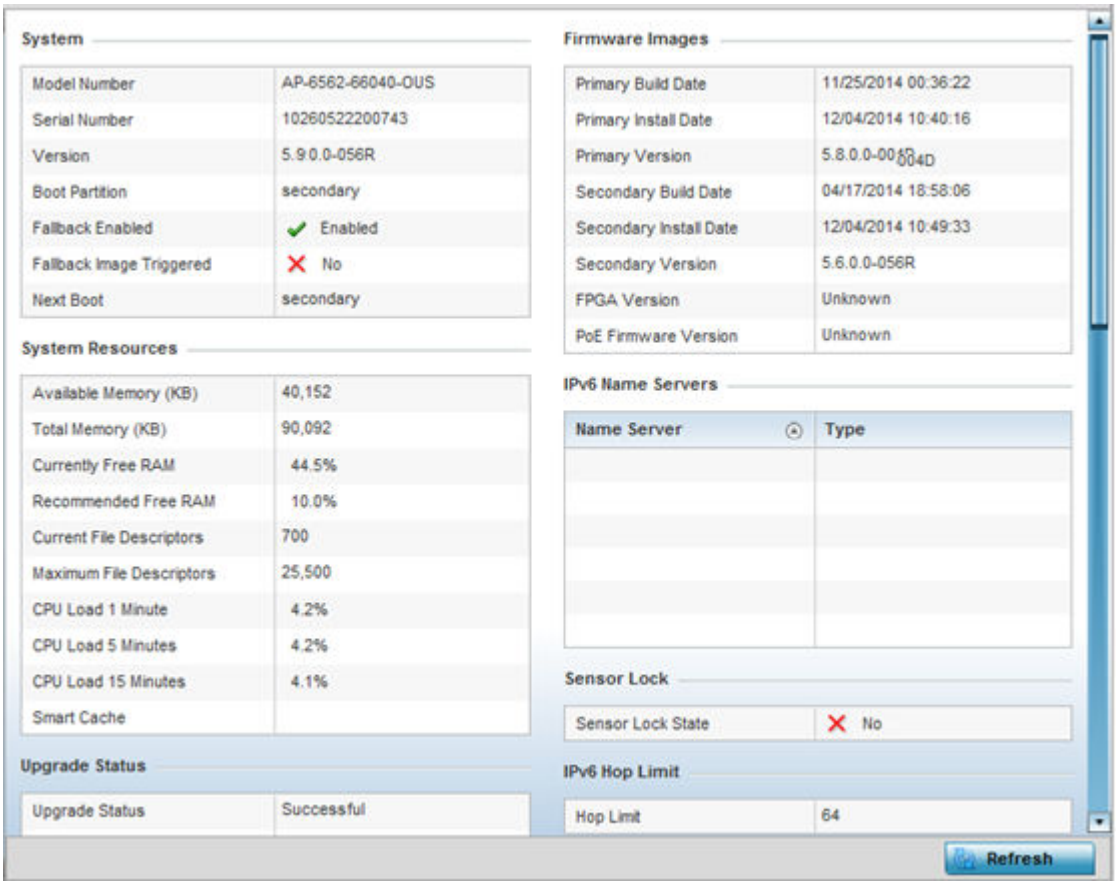
5 Select **Refresh** as needed to update the screen's statistics counters to their latest values.

## AP Device

The Device screen displays basic information about a selected access point. Use this screen to gather version information, boot image utilization and upgrade status. An access point's sensor server capability, power management and system resources can also be administrated from the Device screen.

To view the device statistics:

1 Select the **Statistics** tab from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Select **Device**.




The System field displays the following:

| | |
|---|---|
| Model Number | Displays the model of the selected access point to help distinguish its exact SKU and country of operation. |
| Serial Number | Displays the numeric serial number set for the access point. |
| Version | Displays the software (firmware) version on the access point. Use this information to assess whether a firmware upgrade would enhance the access point's support capability. |
| Boot Partition | Displays the boot partition type. |
| Fallback Enabled | Displays whether this option is enabled. This method enables a user to store a known legacy version and a new version in device memory. The user can test the new software, and use an automatic fallback, which loads the old version on the access point if the new version fails. |
| Fallback Image Triggered | Displays whether the fallback image was triggered. The fallback image is an old version of a known and trusted operational firmware image stored in device memory. This allows a user to test a new version of firmware. If the new version fails, you can use the old version to ensure the access point's duty cycle is maintained. |
| Next Boot | Designates this version as the version used the next time the access point is booted. |

The System Resources field displays the following:

| | |
|---|---|
| Available Memory (MB) | Displays the available memory (in MB) available on the access point. |
| Total Memory (MB) | Displays the access point's total memory. |
| Currently Free RAM | Displays the access point's free RAM space. If its very low, free up some space by closing some processes. |
| Recommended RAM | Displays the recommended RAM required for routine operation. |
| Current File Description | Displays the access point's current file description. |
| Maximum File Description | Displays the access point's maximum file description. |
| CPU Load 1 Minute | Lists this access point's CPU utilization over a 1 minute span. |
| CPU Load 5 Minutes | Lists this access point's CPU utilization over a 5 minute span. |
| CPU Load 15 Minutes | Lists this access point's CPU utilization over a 15 minute span. |

The Fan Speed field displays the following:

| | |
|---|---|
| Number | Displays the number of fans supported on the listed access point. access point models each have unique fan support. |
| Speed (Hz) | Displays the fan speed in Hz. |

The Temperature field displays the following:

| | |
|---|---|
| Number | Displays the number of temperature elements (gauges) used by the access point. |
| Temperature | Displays the current temperature (in Celsius) to assess a potential access point overheat condition. |

The Kernal Buffers field displays the following:

| | |
|---|---|
| Buffer Size | Lists the sequential buffer size. |
| Current Buffers | Displays the current buffers available to the selected access point. |
| Maximum Buffers | Lists the maximum buffers available to the selected access point. |

The IP Domain field displays the following:

| | |
|---|---|
| IP Domain Name | Displays the name of the IP Domain service used with the selected access point. |
| IP Domain Lookup state | Lists the current state of an IP lookup operation. |

The IP Name Servers field displays the following:

| | |
|---|---|
| Name Server | Displays the names of the servers designated to provide DNS resources to this access point. |
| Type | Displays the type of server for each server listed. |

The Firmware Images field displays the following:

| | |
|---|---|
| Primary Build Date | Displays the build date when this access point firmware version was created. |
| Primary Install Date | Displays the date this version was installed. |
| Primary Version | Displays the primary version string. |
| Secondary Build Date | Displays the build date when this version was created. |
| Secondary Install Date | Displays the date this secondary version was installed. |
| Secondary Version | Displays the secondary version string. |
| FPGA Version | Displays whether a FPGA supported firmware load is being utilized. |
| PoE Firmware Version | Displays whether a PoE supported firmware load is being utilized. |

The Sensor Lock field displays the following:

| | |
|---|---|
| Sensor Lock | Displays whether a lock has been applied to access point sensor capabilities. Keeping an access point from performing sensor support ensures client support is continuously maintained. |

The Upgrade Status field displays the following:

| | |
|---|---|
| Upgrade Status | Displays the status of the image upgrade. |
| Upgrade Status Time | Displays the time of the image upgrade. |

The Power Management field displays the following:

| | |
|---|---|
| Power Management Mode | Displays the power mode currently invoked by the selected access point. |
| Power Management Status | Lists the power status of the access point. |
| Ethernet Power Status | Displays the access point's Ethernet power status. |
| Radio Power Status | Displays the power status of the access point's radios. Each access point radio is capable of having a unique, administrator defined, transmit capability. |

The IPv6v Hop Limit table displays the following:

| | |
|---|---|
| Hop Limit | Lists the maximum number of times IPv6 traffic can hop. The IPv6 header contains a hop limit field that controls the number of hops a datagram can be sent before being discarded (similar to the TTL field in an IPv4 header). |

The IPv6 Name Servers field displays the following:

| | |
|---|---|
| Name Server | List the IPv6 name server hosting a network service for providing responses to queries against a directory. The IPv6 name server maps a human recognizable identifier to a system's internal identifier. This service is performed by the server in response to a network service protocol request. |
| Type | Lists the type of IPv6 name server mapping a human readable identifier to system identifier. |

The IPv6 Delegated Prefixes table displays the following:

| | |
|---|---|
| IPv6 Delegated Prefix | In IPv6, prefix delegation is used to assign a network address prefix, configuring the controller or service platform with the prefix. |
| Prefix Name | Lists the name assigned to the IPv6 delegated prefix. |
| DHCPv6 Client State | Displays the current DHCPv6 client state as impacted by the IPv6 delegated prefix. |
| Interface Name | Lists the interface over which IPv6 prefix delegation occurs. |
| T1 timer (seconds) | Lists the amount of time in seconds before the DHCP T1 (delay before renew) timer expires. |
| T2 timer (seconds) | Lists the amount of time in seconds before the DHCP T2 (delay before rebind) timer expires. |
| Last Refreshed (seconds) | Lists the time, in seconds, since IPv6 prefix delegation has been updated. |
| Preferred Lifetime (seconds) | Lists is the time in seconds (relative to when the packet is sent) the IPv6 formatted addresses remains in a preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime. |
| Valid Lifetime (seconds) | Displays the time in seconds (relative to when the packet is sent) the IPv6 formatted address remains in a valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime. |

5 Select **Refresh** to update the statistics counters to their latest values.

## AP Web Filtering

The Web-Filtering screen displays information on Web requests for content and whether the requests were blocked or approved based on URL filter settings defined for the selected access point. A URL filter is comprised of several filter rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

To view Web filter statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

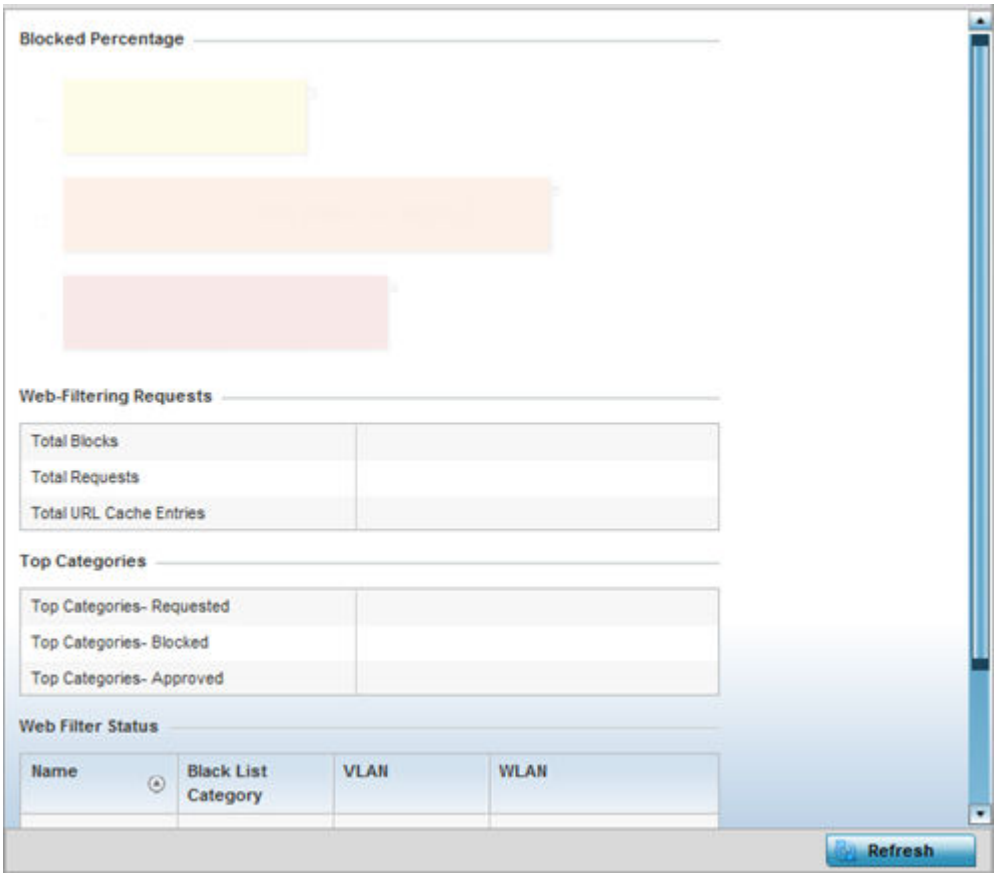
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Web-Filtering**.

The **Statistics > AP > Web-Filtering** screen is displayed.




5 Review the following Web-Filtering statistics:

The Web-Filtering Requests field displays the following information:

| | |
|---|---|
| Total Blocks | Lists the number of Web request hits against content blocked in the URL blacklist. |
| Total Requests | Lists the total number of requests for URL content cached locally on this access point. |
| Total URL Cache Entries | Displays the number of cached URL data entries made on this access point on the request of requesting clients requiring URL data managed by the access point and their respective *whitelist* or *blacklist*. |

The Top Categories field helps administrators assess the content most requested, blocked and approved based on the defined *whitelist* and *blacklist* permissions:

| | |
|---|---|
| Top Categories - Requested | Lists those Web content categories most requested by clients managed by this access point. Use this information to assess whether the permissions defined in the blacklist and whitelist optimally support these client requests for cached Web content. |
| Top Categories - Blocked | Lists those Web content categories blocked most often for requesting clients managed by this access point. Use this information to periodically assess whether the permissions defined in the blacklist and whitelist still restrict the desired cached Web content from requesting clients. Remember, a whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist. |
| Top Categories - Approved | Lists those Web content categories approved most often on behalf of requesting clients managed by this access point. Periodically review this information to assess whether this cached and available Web content still adheres to your organization's standards for client access. |

The Web Filter Status field displays the following information:

| | |
|---|---|
| Name | Displays the name of the filter whose URL rule set has been invoked. |
| Blacklist Category | Lists the blacklist category whose URL filter rule set has caused data to be filtered to a requesting client. Periodically assess whether these rules are still relevant to the data requirements of requesting clients. |
| VLAN | Lists the impacted access point VLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category. |
| WLAN | Lists the impacted access point WLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category. Periodically assess whether clients are segregated to the correct WLAN based on their cached Web data requirements and impending filter rules. |

6 Periodically, select **Refresh** to update this screen to its latest values.

## AP Application Visibility (AVC)

Controllers and service platforms can inspect every byte of each application header packet allowed to pass their managed radio devices. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application.

Note
The WiNG 7.1 release does not support DPI on AP505 and AP510 model access points. This feature will be supported in future releases.

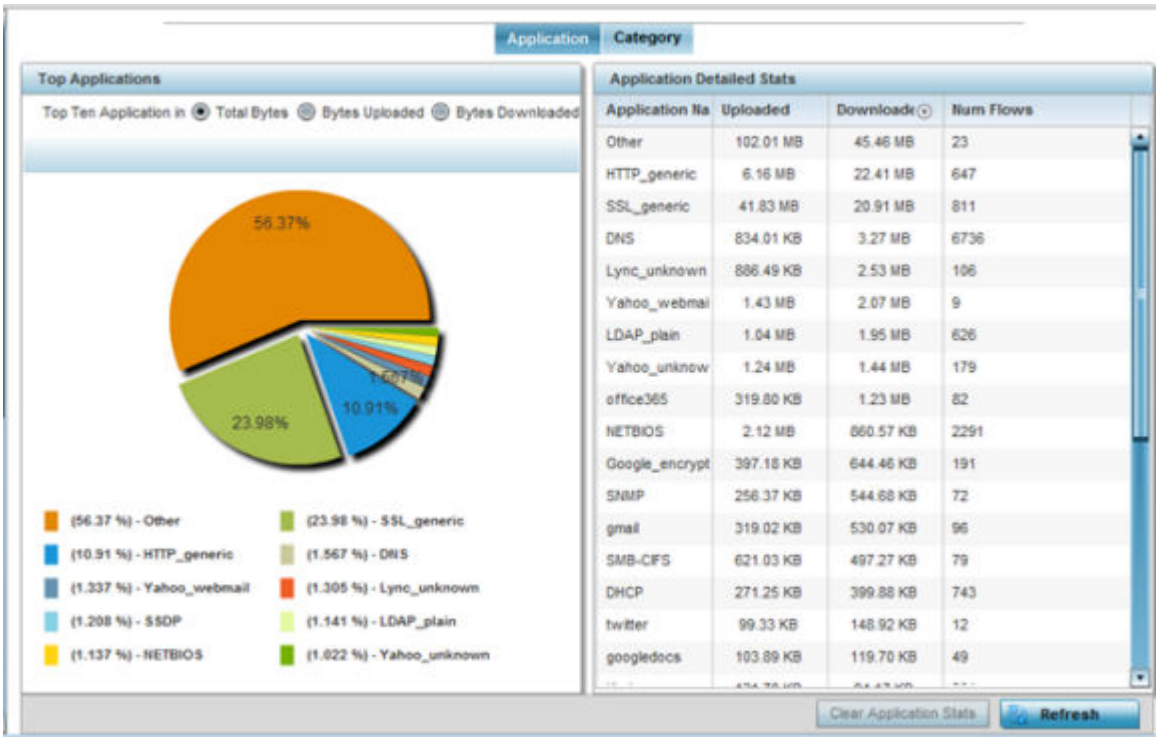
1 Select the **Statistics** → **System** tab from the Web UI.

2 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

3 Select **Application Visibility (AVC)** from the menu.

The **Statistics → AP → Application Visibility (AVC) → Application** screen displays.




4 Refer to the Top Applications graph to assess the most prolific, and allowed, application data passing through the controller/access point managed network.

| | |
|---|---|
| Total Bytes | Displays the top ten utilized applications in respect to total data bytes passing through the access point managed network. These are only the administrator allowed applications approved for proliferation within the access point managed network. |
| Bytes Uploaded | Displays the top ten applications in respect to total data bytes uploaded through the access point managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority). |
| Bytes Downloaded | Displays the top ten applications in respect to total data bytes downloaded from the access point managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority). |

5 Refer to the Application Detailed Stats table to assess specific application data utilization:

| | |
|---|---|
| Application Name | Lists the allowed application name whose data (bytes) are passing through the access point managed network. |
| Uploaded | Displays the number of uploaded application data (in bytes) passing the through the access point managed network. |

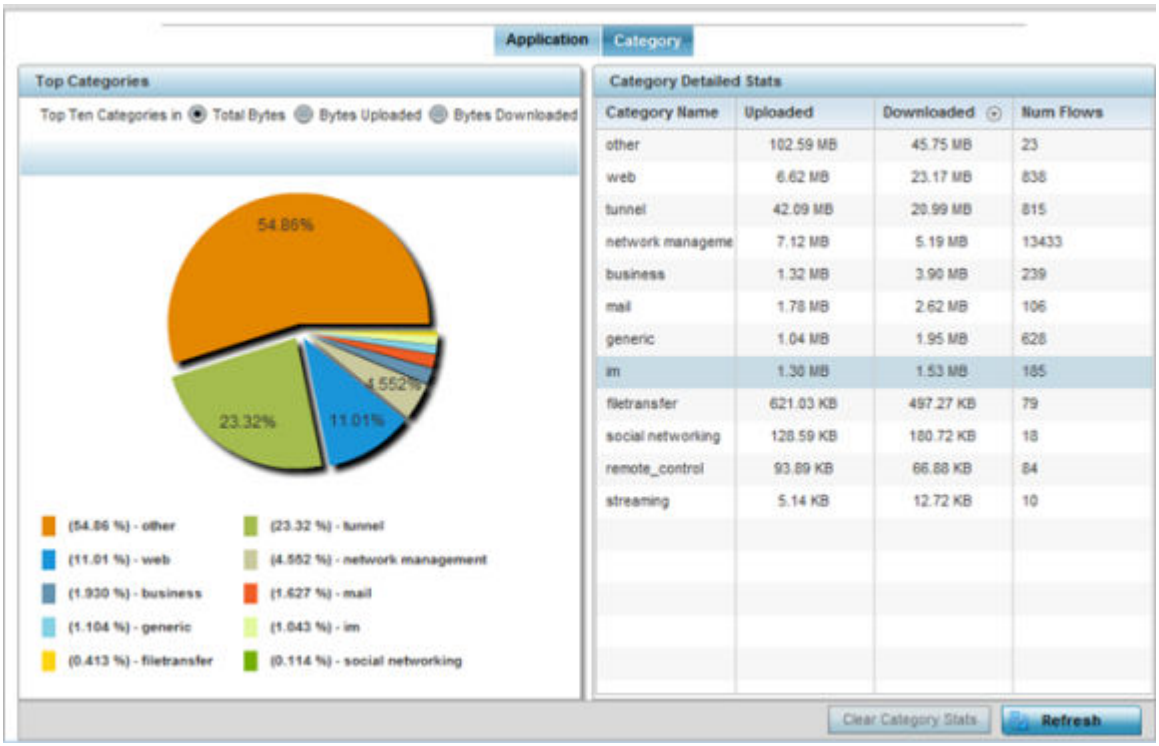
| | |
|---|---|
| Downloaded | Displays the number of downloaded application data (in bytes) passing the through the access point managed network. |
| Num Flows | Lists the total number of application data flows passing through the access point for each listed application. An application flow can consist of packets in a specific connection or media stream. Application packets with the same source address/port and destination address/port are considered one flow. |

6 Click **Clear Application Stats** to clear the application assessment data counters and begin a new assessment. Selecting this option will not clear category stats, just application stats.

7 Click the **Category** tab.

Categories are existing system or user defined application groups (video, streaming, mobile, audio etc.) that assist administrators in filtering (allowing or denying) application data.

The **Statistics > Controller > Application Visibility > Category** screen displays.




Refer to the Top Categories graph to assess the most prolific, and allowed, application data categories utilized by the access point.

| | |
|---|---|
| Total Bytes | Displays the top ten application categories in respect to total data bytes passing through the access point managed network. These are only the administrator allowed application categories approved for proliferation within the access point managed network. |
| Bytes Uploaded | Displays the top ten application categories in respect to total data bytes uploaded through the access point managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority). |
| Bytes Downloaded | Displays the top ten application categories in respect to total data bytes downloaded from the access point managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories and categories or adjusting their precedence (priority). |

Refer to the **Category Detailed Stats** table to assess specific application category data utilization:

| | |
|---|---|
| Category Name | Lists the allowed category whose application data (in bytes) is passing through the access point managed network. |
| Uploaded | Displays the number of uploaded application category data (in bytes) passing the through the access point managed network. |
| Downloaded | Displays the number of downloaded application category data (in bytes) passing the through the access point managed network. |
| Num Flows | Lists the total number of application category data flows passing through access point connected clients. A category flow can consist of packets in a specific connection or media stream. Packets with the same source address/port and destination address/port are considered one flow. |

8 Click **Clear Category Stats** to clear the application category assessment data counters and begin a new assessment. Selecting this option will not clear application stats, just category stats.

9 Click **Refresh** to update the statistics counters to their latest values.

## AP Application Policy

When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. An application policy defines the rules or actions executed on recognized HTTP (Facebook), enterprise (Webex) and peer-to-peer (gaming) applications or application-categories.

For each rule defined, a precedence is assigned to resolve conflicting rules for applications and categories. A deny rule is exclusive, as no other action can be combined with a deny. An allow rule is redundant with other actions, since the default action is allow. An allow rule is useful when wanting to deny packets for a category, but wanting to allow a few applications in the same category to proceed. In such a cases, add an allow rule for applications with a higher precedence then a deny rule for that category.

Mark actions mark packets for a recognized application and category with DSCP/8021p values used for QoS. Rate-limits create a rate-limiter applied to packets recognized for an application and category. Ingress and egress rates need to be specified for the rate-limiter, but both are not required. Mark and

rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

**Note**
The WiNG 7.1 release does not support PPPoE on AP505 and AP510 model access points. This feature will be supported in future releases.

1 Select the **Statistics** tab from the Web UI.
2 Expand the **System** node on the top, left-hand side of the screen.

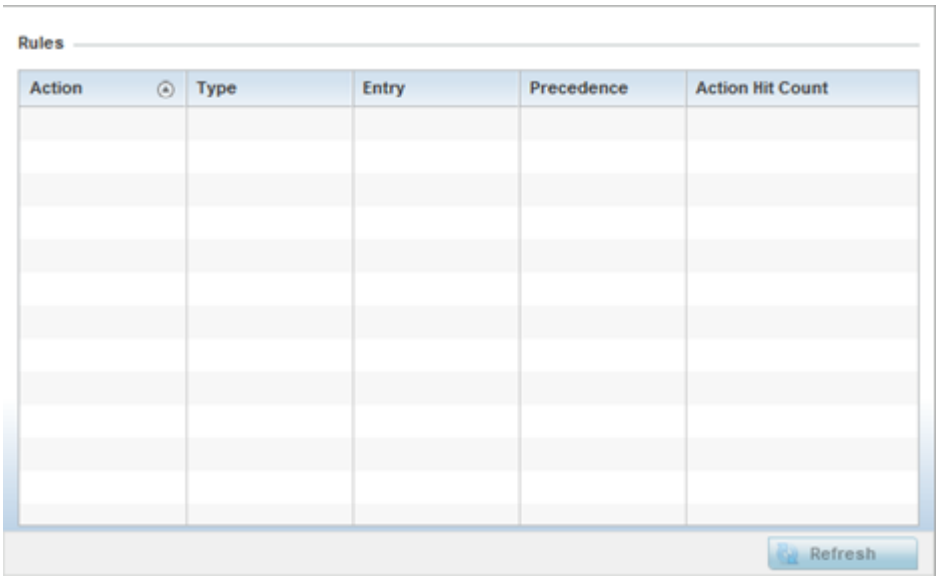
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **Application Policy** from the menu.

The **Statistics → AP → Applcation Policy** screen displays.




5 Refer to the **Rules** table to review the results of the application policies put in place thus far from this managing access point.

| | |
|---|---|
| Action | Displays the action executed on the listed application.<br>• **Allow** - Allows packets for a specific application and its defined category type (social networking etc.). This is the default setting.<br>• **Deny** - Denies (restricts) the action applied to a specific application or a specific application category.<br>• **Mark** - Marks recognized packets with DSCP/8021p value Rate-limit - Rate limits packets from specific application types. |
| Type | Displays the application policy type applied. |
| Precedence | Lists the priority (from 1 - 256) for the application policy rule. The lower the value, the higher the priority assigned to this rule's enforcement action and the category and application assigned. A precedence also helps resolve conflicting rules for applications and categories. |

| | |
|---|---|
| Action Hit Count | Displays the number of times each listed application policy action has been triggered. |

6 Select **Refresh** to update the statistics counters to their latest values.

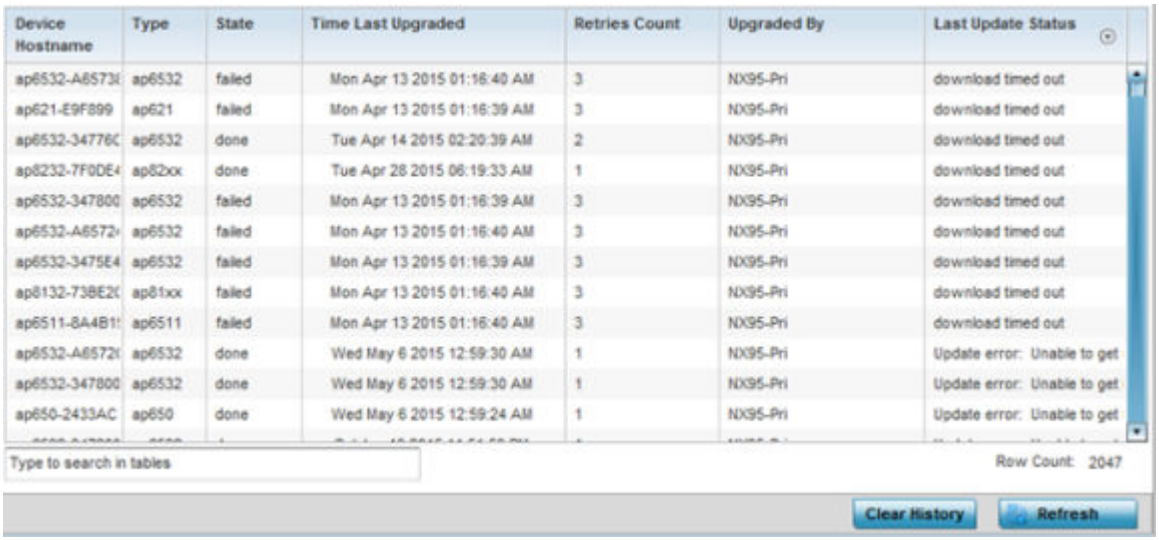
## AP Device Upgrade

The Device Upgrade screen displays information about devices receiving updates and those devices to perform an update. Use this screen to gather version data, install firmware images, boot an image and upgrade status.

To view the device upgrade statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Select **Device Upgrade**.

The AP Upgrade statistics screen is displayed.




This screen displays the following:

| | |
|---|---|
| Device Hostname | Displays the administrator-assigned hostname of the access point receiving the update. |
| Type | Displays the model type of the access point receiving a firmware update. |
| State | Displays the current state of the upgrade process (**`done`**, **`failed`**, etc.). |
| Time Last Upgraded | Displays the date and time of the last successful access point upgrade operation. |
| Retries Count | Displays the number of retries made in an access point update operation. |
| Upgraded By | Displays the MAC address of the access point that performed the upgrade. |
| Last Update Status | Displays the status of the last upgrade operation (**`Start Upgrade`**, **`Update error`**, etc.). |

5 Select **Clear History** to clear the screen of its current status and begin a new data collection.
6 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Adoption

Access point adoption stats are available for both currently adopted and access points pending adoption. Historical data can be also be fetched for adopted access points.

Adoption is the process an access point uses to discover available controllers, or Controller APs of the same model, pick the most desirable one, establish a connection and obtain its configuration to adequately provision itself.

For more information, refer to the following:

- Adopted APs
- AP Adoption History
- AP Self Adoption History
- Pending Adoptions

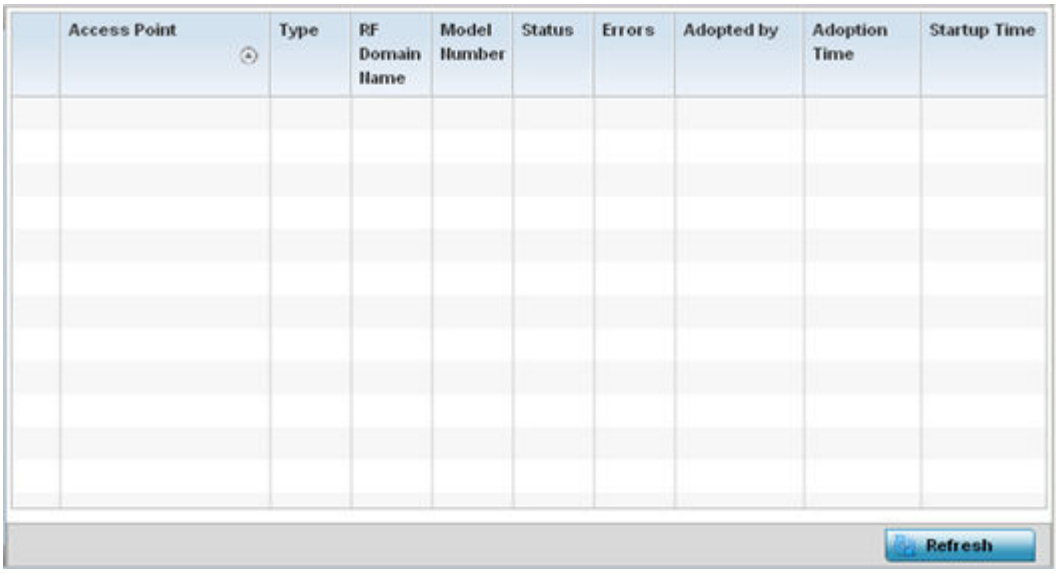
### *Adopted APs*

The Adopted APs screen lists access points adopted by the selected access point, their RF Domain memberships and network service information.

To view adopted access point statistics:

1 Select the **Statistics** tab from the Web UI.
2 Expand the **System** from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **Adoption** menu.

The **Adoption > Adopted APs** screen displays by default.




This screen displays the following:

| | |
|---|---|
| Access Point | Displays the name assigned to the adopted access point as part of its device configuration. |
| Type | Displays each listed access point's model type |
| RF Domain Name | Displays each access point's RF Domain membership. An access point can only share RF Domain membership with other access points of the same model. |
| Model Number | Displays each listed access point's model number |
| Config Status | Displays each listed access point's configuration status to help determine its service role. |
| Config Errors | Lists any configuration errors that may be hindering a clean adoption. |
| Adopted By | Lists the adopting access point. |
| Adoption Time | Displays each listed access point's time of adoption. |
| Startup Time | Displays each listed access point's in-service time since last offline. |

5 Select **Refresh** to update the screen's statistics counters to their latest values..

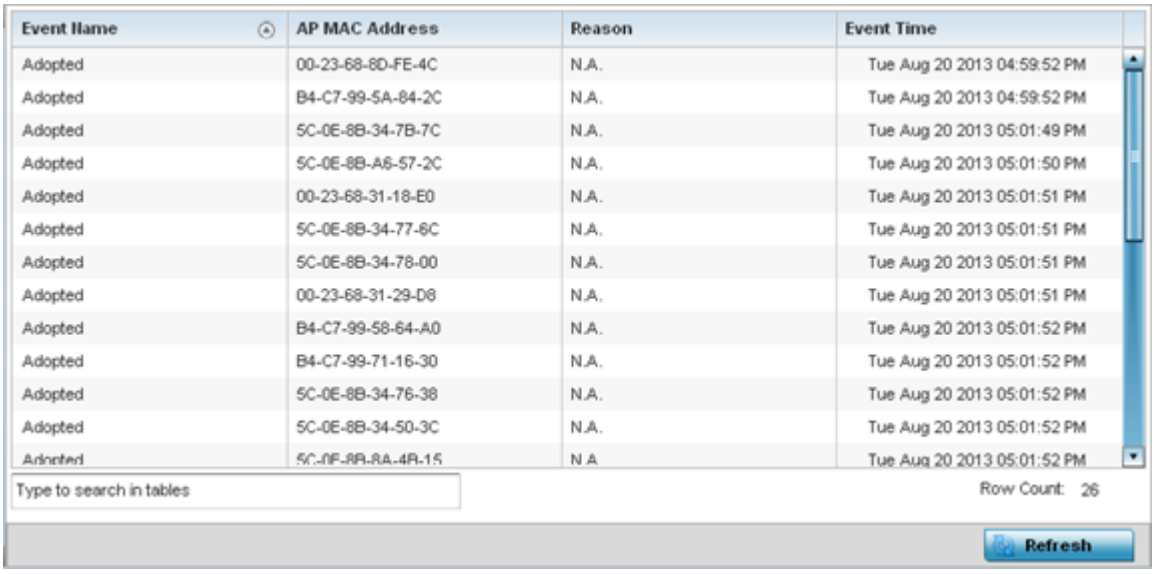
*AP Adoption History*

An **AP Adoption History** screen displays a list of peer access points and their adoption event status.

To view historical statistics for adopted access points:

1 Select the **Statistics** tab from the Web UI.
2 Expand the **System** from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Adoption** menu.
5 Select **AP Adoption History**.

The **Adoption > Adoption History** screen is displayed.




This screen describes the following historical data for adopted access points:

| | |
|---|---|
| Event Name | Displays the adoption status of each listed access point as either **`adopted`** or **`un-adopted`**. |
| AP MAC Address | Displays the MAC address of each access point this access point has attempted to adopt. |
| Reason | Displays the reason code for each event listed in the adoption history table. |
| Event Time | Displays day, date and time for each access point adoption attempt. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

### *AP Self Adoption History*

The AP Self Adoption History displays an event history of peer access points that have adopted to the selected access point.

1 Select the **Statistics** tab from the Web UI.

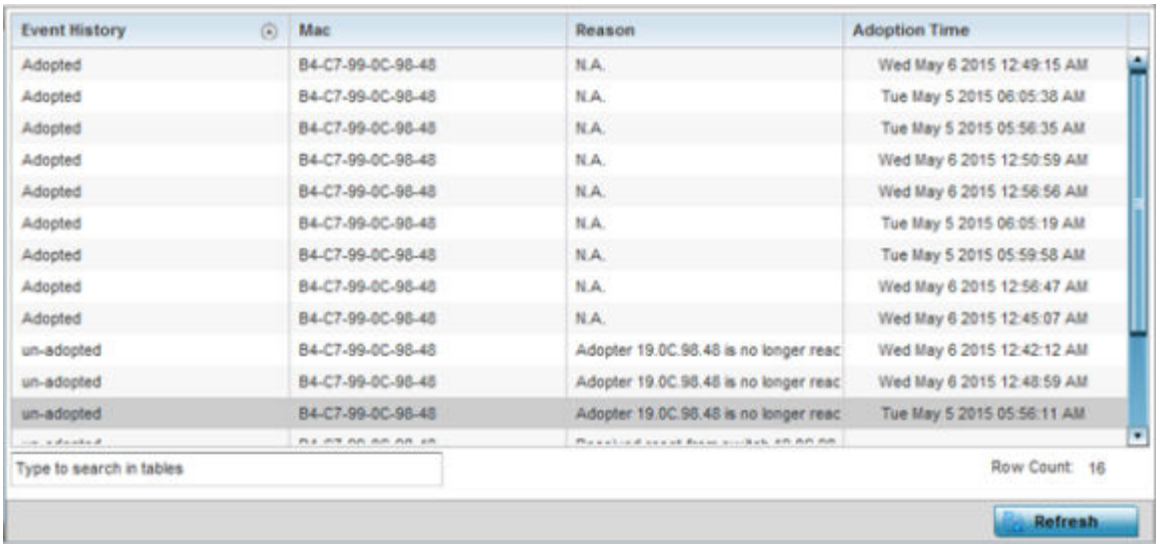
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Adoption** menu.

5 Select **AP Self Adoption History**.

The **Adoption > AP Self Adoption History** screen is displayed.




This screen describes the following historical data for adopted access points:

| | |
|---|---|
| Event History | Displays the self adoption status of each AP as either **`Adopted`** or **`un-adopted`**. |
| MAC | Displays the MAC of the auto adopted access point. |
| Reason | Displays the adoption reason code for an access point's auto adoption. |
| Adoption Time | Displays a timestamp for the access point's auto-adoption. |

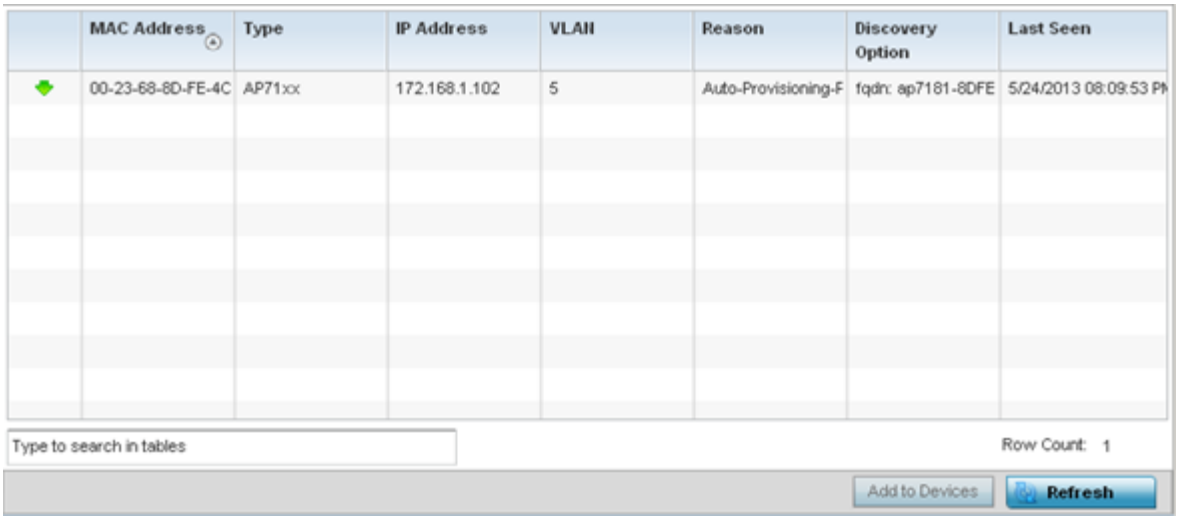
6 Select **Refresh** to update the screen's statistics counters to their latest values.

### *Pending Adoptions*

The **Pending Adoptions** screen displays a list of devices yet to be adopted to this access point and access points still in the process of adoption.

To view pending access point statistics:

1 Select the **Statistics** tab from the Web UI.
2 Expand the **System** from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Adoption** menu.
5 Select **Pending Adoptions**.




This screen displays the following information:

| | |
|---|---|
| MAC Address | Displays the MAC address of the device pending adoption. |
| Type | Displays the AP model type. access points can only adopt others of the same model, as their radio configurations differ by model. |
| IP Address | Displays the current IP Address of the device pending adoption. |
| VLAN | Displays the current VLAN used as a virtual interface by device pending adoption. |
| Reason | Displays the status as to why the device is still pending adoption and has not yet successfully connected to this access point. |
| Discovery Option | Displays the discovery option code for each AP listed pending adoption. |
| Last Seen | Displays the date and time stamp of the last time the device was seen. Click the arrow next to the date and time to toggle between standard time and UTC. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

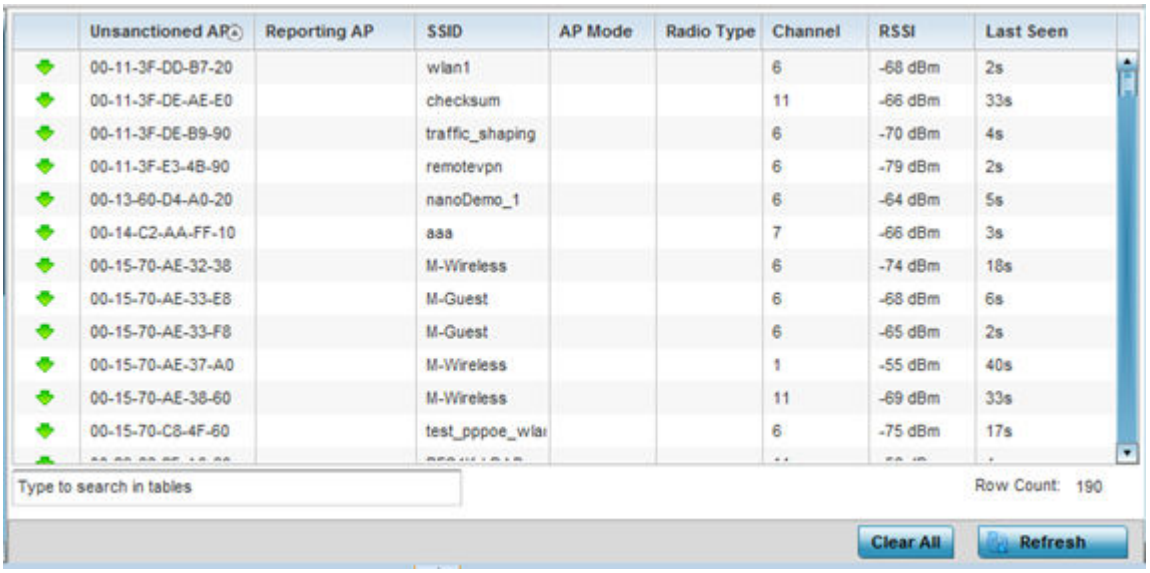
## AP Detection

The AP Detection screen displays potentially hostile access points, their SSIDs, reporting AP, and so on. Continuously re-validating the credentials of detected devices reduces the possibility of an access point hacking into the network.

To view the AP detection statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Select **AP Detection**.

The **Statistics > Access Point > AP Detection** screen displays.




This screen displays the following:

| | |
|---|---|
| Unsanctioned AP | Displays the MAC address detected access points that are yet to be authorized for interoperability within the access point managed network. |
| Reporting AP | Displays the hardware encoded MAC address of the radio used by the detecting access point. Select an access point to display configuration and network address information in greater detail. |
| SSID | Displays the WLAN SSID the unsanctioned access point was detected on. |
| AP Mode | Displays the operating mode of the unsanctioned access point. |
| Radio Type | Displays the type of the radio on the unsanctioned access point. The radio can be *802.11b*, *802.11bg*, *802.1bgn*, *802.11a* or *802.11an*. |
| Channel | Displays the channel the unsanctioned access point is currently transmitting on. |
| Last Seen | Displays the time (in seconds) the unsanctioned access point was last seen on the network. |
| RSSI | Lists a RSSI *(relative signal strength indication)* for a detected (and perhaps unsanctioned) access point. |

5 T

6 Select **Clear All** to clear the screen of its current status and begin a new data collection.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Wireless Clients

The Wireless Clients screen displays credential information for wireless clients associated with an access point. Use this information to assess if configuration changes are required to improve network performance. Clients can be selected from amongst those displayed to display the client's configuration in greater detail.

To view wireless client statistics:

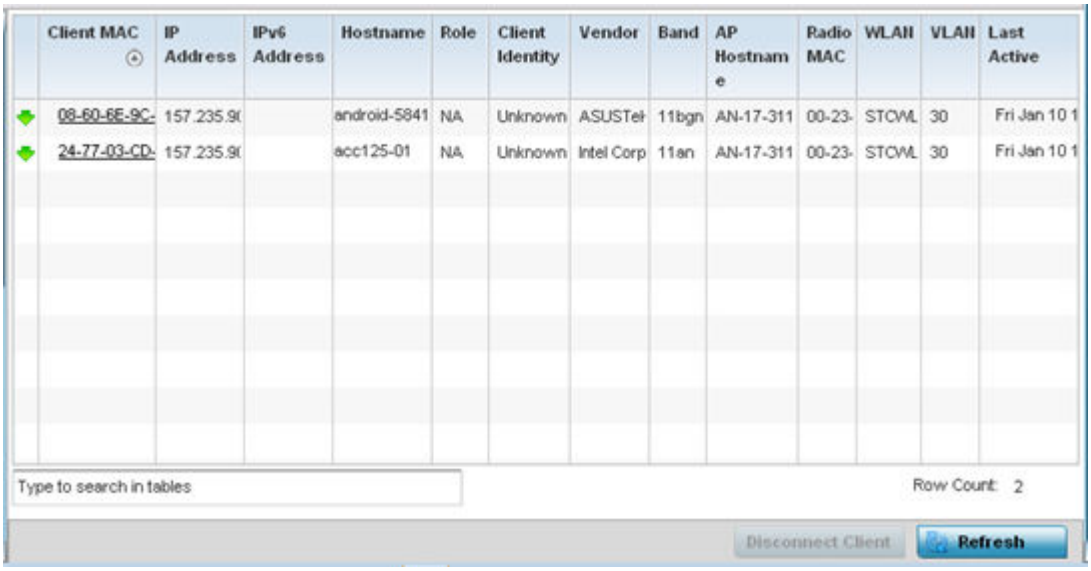
1 Select the Statistics menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **Wireless Clients**.

The **Statistics → Access Point → Wireless Client** screen displays.




This screen displays the following information:

| | |
|---|---|
| Client MAC | Lists the factory encoded hardware identifier for each listed client. The MAC address displays as a link that can be selected to display individual client configuration and network address information in greater detail. |
| IP Address | Displays the unique IP address of the client. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval. |
| IPv6 Address | Displays the current IPv6 formatted IP address a listed guest client is using as a network identifier. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Hostname | Displays the hostname (MAC addresses) of connected wireless clients. The hostname displays as a link that can be selected to display configuration and network address information in greater detail. |
| Role | Lists the client's defined role within the access point managed network. |
| Client Identity | Displays the unique Client Identity of this device. |
| Vendor | Lists the name of the manufacturer (hardware vendor) of each listed client to help assess its compatibility with the WiNG managed wireless infrastructure. |
| Band | Displays the 802.11 radio band on which the listed wireless client operates. |
| AP Hostname | Displays the administrator assigned name applied to the access point detecting the listed client. |
| Radio MAC | Lists the factory encoded hardware identifier assigned to the detecting access point radio. |
| WLAN | Displays the name of the WLAN the access point's using with each listed client. Use this information to determine if the client's WLAN assignment best suits its intended deployment in respect to the WLAN's QoS objective. |

| | |
|---|---|
| VLAN | Displays the VLAN ID each listed client is currently mapped to as a virtual interface for access point interoperability. |
| Last Active | Displays a time stamp when the detected client was last observed within the network. |

5 Select a specific client MAC address and select **Disconnect Client** to terminate this client's connection and RF Domain membership.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

7 The Wireless Clients screen displays the following:

## AP Wireless LANs

The Wireless LANs screen displays an access point WLAN utilization. This screen displays access point WLAN assignments, SSIDs, traffic utilization, WLAN radio utilization and transmit and receive statistics.

To review a selected access point's WLAN statistics:

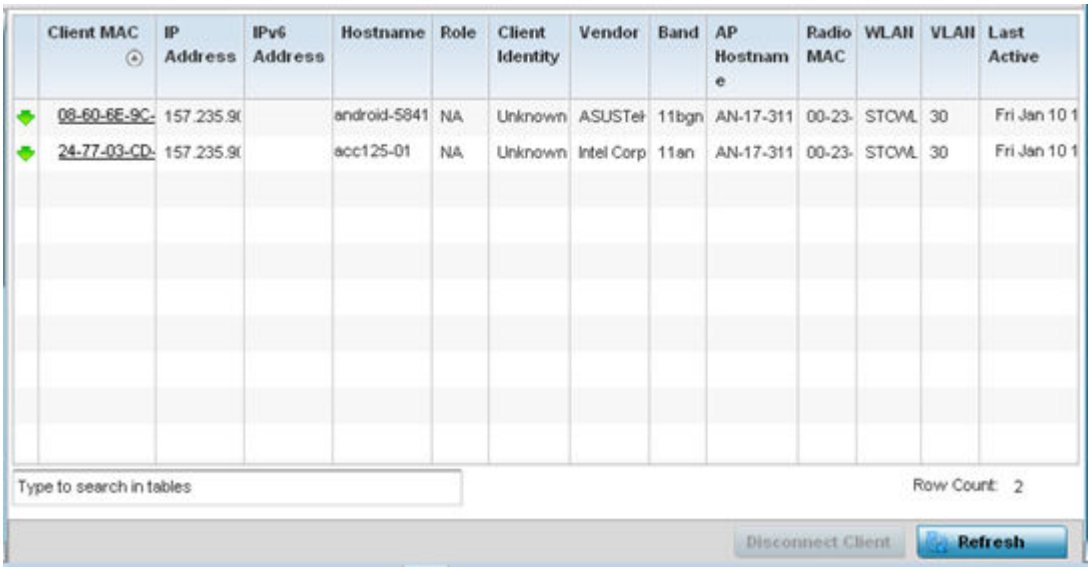
1 Select the Statistics menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Wireless LANs**.

The **Statistics > Access Point > Wireless WLANs** screen displays.




This screen displays the following:

| | |
|---|---|
| WLAN Name | Displays the name of the WLAN the access point is currently using for client support and QoS configuration segregation (voice versus data etc.). |
| SSID | Displays each listed WLAN's SSID. |

| | |
|---|---|
| Traffic Index | Displays the traffic utilization index, which measures how efficiently the WLAN's traffic medium is used. It's defined as the percentage of current throughput relative to maximum possible throughput. Low indexes may require administration to assess why there's an excess of missed packets.<br>Traffic indices are:<br>• *0 – 20* (very low utilization)<br>• *20 – 40* (low utilization)<br>• *40 – 60* (moderate utilization)<br>• *60 and above* (high utilization) |
| Radio Count | Displays the cumulative number of peer access point radios deployed within each listed WLAN. |
| Tx Bytes | Displays the total number of transmitted bytes on each listed WLAN. |
| Tx User Data Rate | Displays the user data rate in kbps for each listed WLAN. |
| Rx Bytes | Displays the total number of packets (in bytes) received on each listed WLAN. |
| Rx User Data Rate | Displays the received user data rate on each listed WLAN. |

5 Select an WLAN then **Disassociate All Clients** to terminate each client connection within that WLAN.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Policy Based Routing

The Policy Based Routing screen displays statistics for selective PBR *(path packet redirection)*. PBR can optionally mark traffic for preferential services (QoS). PBR is applied to incoming routed packets, and a route-map is generated containing filters and associated redirection actions. Based on the actions defined in the route-map, packets are forwarded to the next relevant hop. Route-maps are configurable under a global policy called *routing-policy*, and applied to profiles and devices.

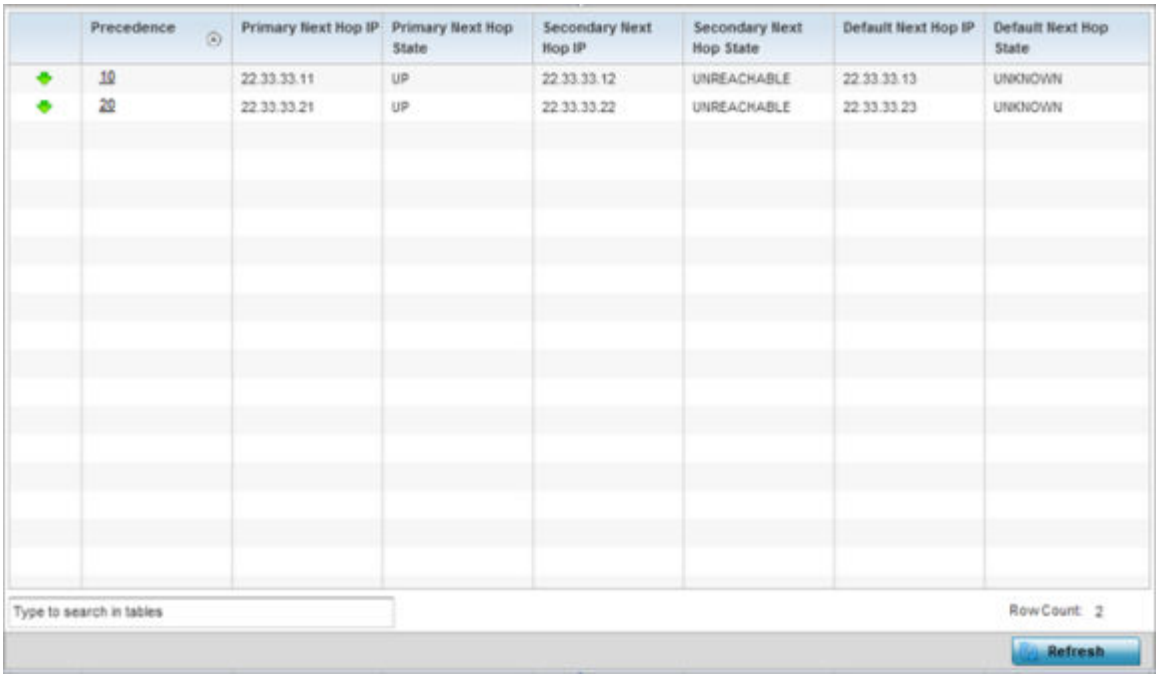
To review access point PBR statistics:

1 Select the Statistics menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Policy Based Routing.**




This screen displays the following:

| | |
|---|---|
| Precedence | Lists the numeric precedence (priority) assigned to each listed PBR configuration. A route-map consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value). |
| Primary Next Hop IP | Lists the IP address of the virtual resource that, if available, is used with no additional route considerations. |
| Primary Next Hop State | Displays whether the primary hop is applied to incoming routed packets. |
| Secondary Next Hop IP | If the primary hop is unavailable, a second redirection resource is used. This column lists the address set for the alternate route in the election process. |
| Secondary Next Hop State | Displays whether the secondary hop is being applied to incoming routed packets. |
| Default Next Hop IP | If a packet subjected to PBR does not have an explicit route to its destination, the pre-set next hop is used. This is either the IP address of the next hop or the outgoing interface. Only one default next hop is available. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reverse. |
| Default Next Hop State | Displays whether the default hop is being applied to incoming routed packets. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Radios

The **Radio** statistics screens display information on access point radios. The actual number of radios depend on the access point model and type. The radio statistics screens display information on a per radio basis. Use this information to refine and optimize the performance of each radio and improve client throughput.

The access point's radio statistics screens detail associated radio ID, type, RF quality index etc. Use this information to assess the overall health of radio transmissions and access point deployment accuracy.

Each of these screens provide enough statistics to troubleshoot issues related to the following three areas:

- AP Radio Status on page 997
- AP Radio RF Statistics on page 998
- AP Radio Traffic Statistics on page 999

Individual access point radios display as selectable links within each of the three radio screens. To review a radio's configuration in greater detail, select the link within the Radio column. Use the Details screen to review this radio's configuration in greater detail, as additional deployment location, configuration, Smart RF, quality index and wireless client information becomes available.

Additionally, navigate the *Traffic*, *WMM TSPEC*, *Wireless LANs* and *Graph* options available on the upper, left-hand side, of the screen to review radio traffic utilization, WMM QoS settings, WLAN advertisement and radio graph information in greater detail. This information can help determine whether the radio is properly configured in respect to its intended deployment objective.

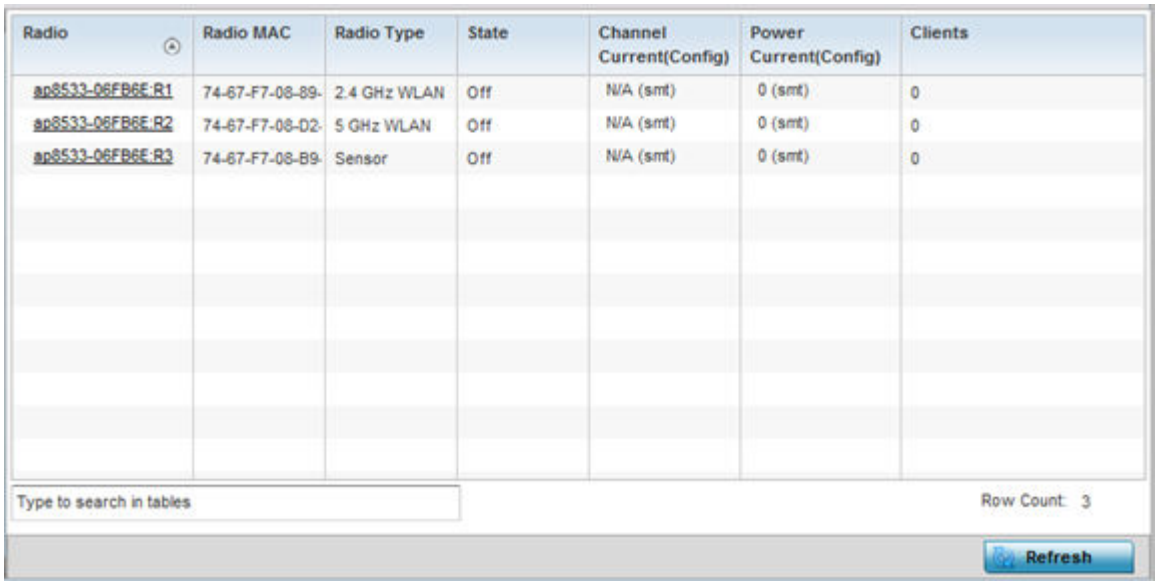
### *AP Radio Status*

Use the Status screen to review access point radio stats in detail. Optionally select individual and access points and launch sub screens with granular performance data. Review radios, operational states, channel utilization and power consumption to assess whether a radio is optimally configured or physically deployed..

To view access point radio statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **Radios** menu.

The **Statistics > Access Point > Radios > Status** screen displays by default.




This screen displays the following:

| | |
|---|---|
| Radio | Displays the administrator assigned radio name as its unique identifier. The name displays in the form of a link that can be selected to launch a detailed screen containing radio throughout data in greater detail. |
| Radio MAC | Displays the factory encoded hardware MAC address assigned to the radio. |
| Radio Type | Displays the radio as either supporting the 2.4 or 5 GHZ radio band. |
| State | Lists a radio's On/Off operational designation. |
| Channel Current (Config) | Displays the configured channel each listed radio is set to transmit and receive on. Use this information to assess whether a channel adjustment has been made (by Smart RF) to compensate for a failed peers client load on a different channel. |
| Power Current (Config) | Displays the configured power each listed radio is using to transmit and receive. Use this information to periodically assess whether a power adjustment has been made (by Smart RF) to compensate for a failed peer radio. |
| Clients | Displays the number of connected clients currently utilizing the listed access point radio. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

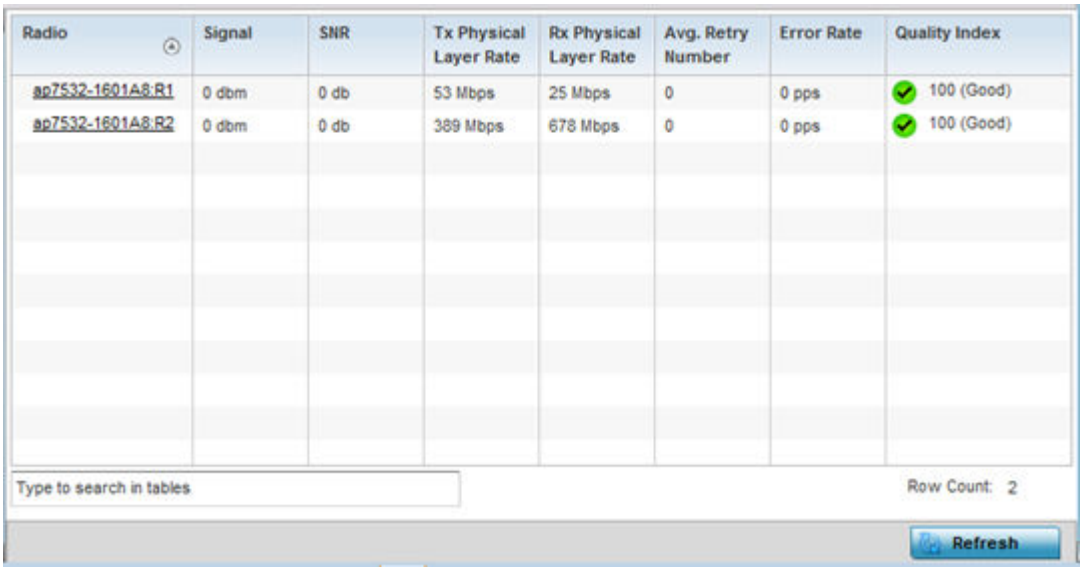
### *AP Radio RF Statistics*

Use the **RF Statistics** screen to review access point radio transmit and receive statistics, error rate and RF quality.

To view access point radio RF statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Radios** menu.
5 Select **RF Statistics**.

The **Statistics > access point > Radios > RF Statistics** screen displays.




This screen displays the following:

| | |
|---|---|
| Radio | Displays the name assigned to the radio as its unique identifier. The name displays in the form of a link that can be selected to launch a detailed screen containing radio throughout data. |
| Signal | Displays the radio's current power level in - dBm. |
| SNR | Displays the SNR *(signal to noise ratio)* of the radio's associated wireless clients. |
| Tx Physical Layer Rate | Displays the data transmit rate for the radio's physical layer. The rate is displayed in Mbps. |
| Rx Physical Layer Rate | Displays the data receive rate for the radio's physical layer. The rate is displayed in Mbps. |
| Avg Retry Number | Displays the average number of retries per packet. A high number indicates possible network or hardware problems. Assess the error rate in respect to potentially high signal and SNR values to determine whether the error rate coincides with a noisy signal. |
| Error Rate | Displays the total number of received packets which contained errors for the listed radio. |
| Traffic Index | Displays the traffic utilization index of the radio. This is expressed as an integer value. 0 – 20 indicates very low utilization, and 60 and above indicate high utilization. |
| Quality Index | Displays an integer that indicates overall RF performance. The RF quality indices are:<br>• *0 – 50* (poor)<br>• *50 – 75* (medium)<br>• *75 – 100* (good) |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

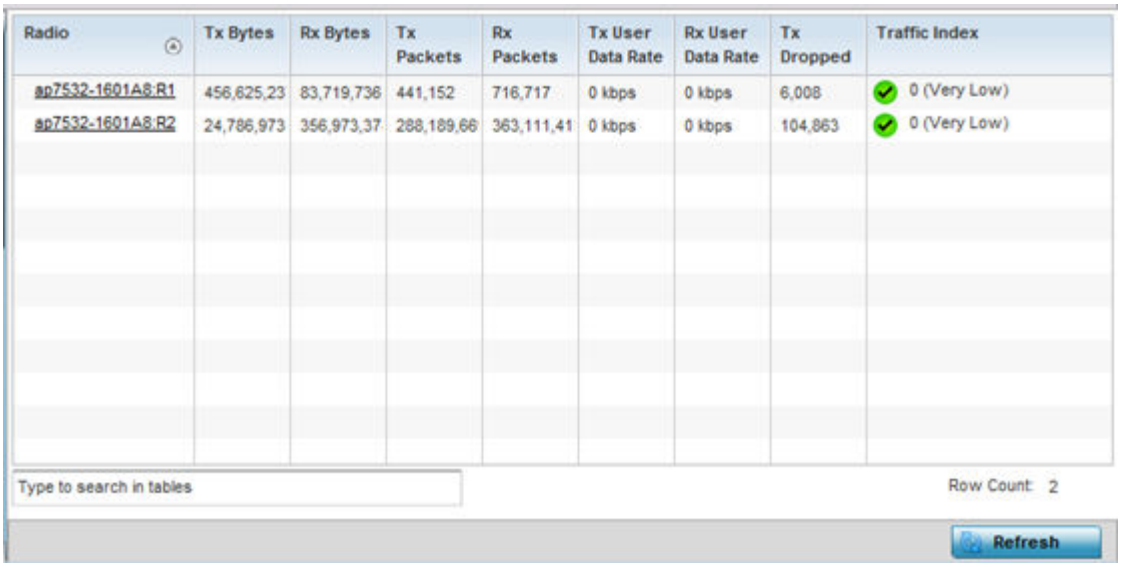
### *AP Radio Traffic Statistics*

Refer to the **Traffic Statistics** screen to review access point radio transmit and receive statistics, data rate and dropped packets during both transmit and receive operations.

To view the access point radio traffic statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Radios** menu.
5 Select **Traffic Statistics**.

The **Statistics > Access Point > Radios > Traffic Statistics** screen displays by default.




This screen displays the following:

| | |
|---|---|
| Radio | Displays the name assigned to the radio as its unique identifier. The name displays in the form of a link that can be selected to launch a detailed screen containing radio throughout data. |
| Tx Bytes | Displays the total number of bytes transmitted by each listed radio. This includes all user data as well as any management overhead data. |
| Rx Bytes | Displays the total number of bytes received by each listed radio. This includes all user data as well as any management overhead data. |
| Tx Packets | Displays the total number of packets transmitted by each listed radio. This includes all user data as well as any management overhead packets. |
| Rx Packets | Displays the total number of packets received by each listed radio. This includes all user data as well as any management overhead packets. |
| Tx User Data Rate | Displays the rate (in kbps) user data is transmitted by each listed radio. This rate only applies to user data and does not include management overhead. |
| Rx User Data Rate | Displays the rate (in kbps) user data is received by the radio. This rate only applies to user data and does not include management overhead. |
| Tx Dropped | Displays the total number of transmitted packets dropped by each listed radio. This includes all user data as well as management overhead packets that were dropped. |
| Error Rate | Displays the total number of received packets which contained errors for the listed radio. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Mesh

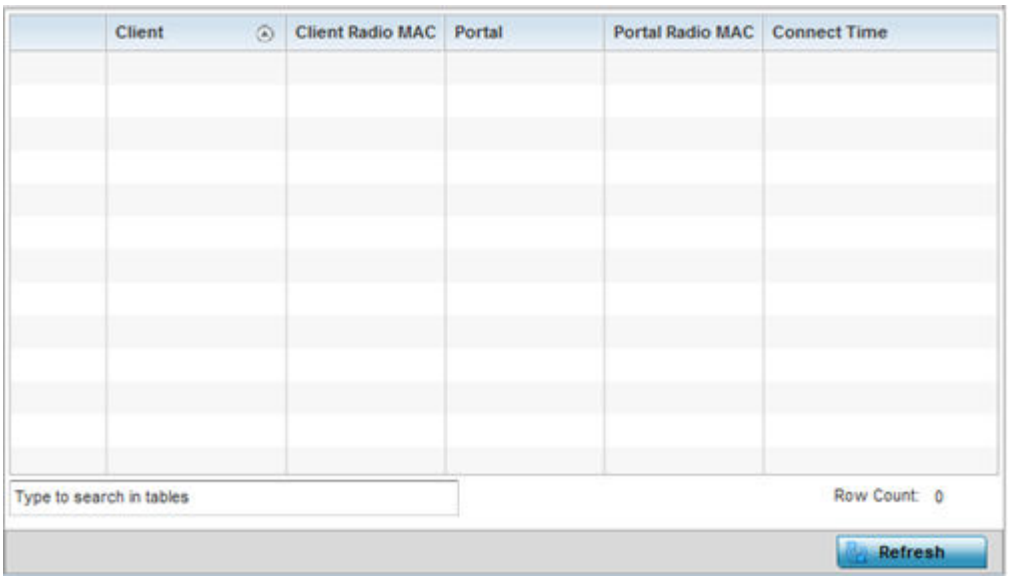
The **Mesh** screen provides detailed statistics on each Mesh capable client available within the selected access point's radio coverage area.

**Note**
The WiNG 7.1 release does not support MeshConnex on AP505 and AP510 model access points. This feature will be supported in future releases.

To view the Mesh statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **Mesh** from the statistics menu.

The **Statistics > AP > Mesh screen** displays.




This screen displays the following:

| | |
|---|---|
| **Client** | Displays the system assigned name of each client connected to a mesh point radio. |
| **Client Radio MAC** | Displays the MAC address of each client radio in the mesh network. |
| **Portal** | Mesh points connected to an external network and forward traffic in and out are Mesh Portals. Mesh points must find paths to a Portal to access the Internet. When multiple Portals exist, the mesh point must select one. |
| **Portal Radio MAC** | Lists the MAC addresses of those access points serving as portals within the mesh network. |
| **Connect Time** | Displays the elapsed connection time for each listed client in the mesh network. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Interfaces

The **Interface** screen provides detailed statistics on each of the interfaces available on the selected access point. Use this screen to review the statistics for each interface. Interfaces vary amongst supported access point models.

Use the following screens to review the configuration of each unique access point model interface:

- AP Interface General Statistics on page 1002
- AP Interface IPv6 Address on page 1005
- AP Interface Multicast Groups Joined on page 1008
- AP Interface Network Graph on page 1009

### *AP Interface General Statistics*

The **General** screen provides information on a selected access point interface such as its MAC address, type and TX/RX statistics.

To view the general interface statistics:

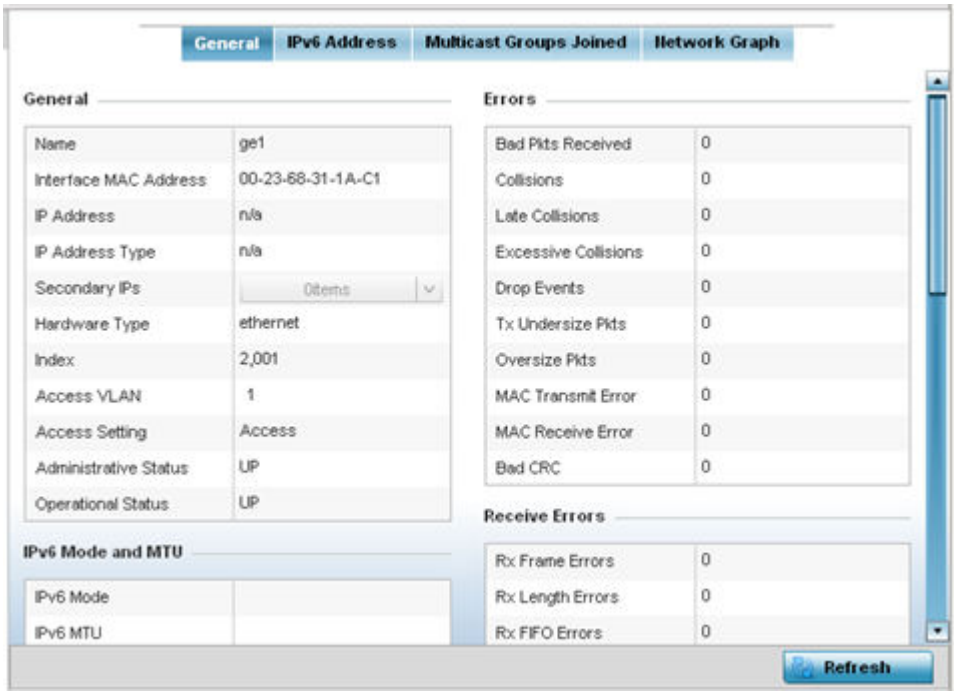
1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **Interfaces** menu.

The **Statistics > AP > Interface > General** screen displays.




5 Select an access point interface from those available for the selected model. The subsequent display within the **`General`** and **`Network Graph`** tabs is specific to the selected model and interface.

The General field describes the following:

| | |
|---|---|
| Name | Displays the name of the access point interface **ge1**, **vlan1**, etc. |
| Interface MAC Address | Displays the MAC address of the access point interface. |
| IP Address | IP address of the interface. |
| IP Address Type | Displays the IP address type, either **IPv4** or **IPv6**. |
| Secondary IP | Displays a list of secondary IP resources assigned to this interface. |
| Hardware Type | Displays the hardware connected type of the interface. |
| Index | Displays the unique numerical identifier supporting the interface. |
| Access VLAN | Displays the tag assigned to the native VLAN. |
| Access Setting | Displays the mode of the VLAN as either **Access** or **Trunk**. |
| Administrative Status | Displays whether the interface is currently **UP** or **DOWN**. |
| Operational Status | Lists whether the selected interface is currently **UP** (operational) or **DOWN**. |

The IPv6 Mode and MTU table displays the following:

| | |
|---|---|
| IPv6 Mode | Lists the current IPv6 mode utilized. |
| IPv6 MTU | Lists the IPv6 formatted largest packet size that can be sent over this interface. |

The Specification field displays the following:

| | |
|---|---|
| Media Type | Displays the physical connection type of the interface.<br>Medium types include:<br>**Copper** - Used on RJ-45 Ethernet ports<br>**Optical** - Used on fibre optic gigabit Ethernet ports |
| Protocol | Displays the routing protocol used by the interface. |
| MTU | Displays the MTU *(maximum transmission unit)* setting configured on the interface. The MTU value represents the largest packet size that can be sent over a link. 10/100 Ethernet ports have a maximum setting of 1500. |
| Mode | The mode can be either:<br>• **Access** – This Ethernet interface accepts packets only from the native VLANs.<br>• **Trunk** – This Ethernet interface allows packets from a list of VLANs you can add to the trunk. |
| Metric | Displays the metric associated with the interface's route. |
| Maximum Speed | Displays the maximum speed the interface uses to transmit or receive data. |
| Admin. Speed | Displays the speed the port can transmit or receive. This value can be either **10**, **100**, **1000** or **Auto**. This value is the maximum port speed in Mbps. Auto indicates the speed is negotiated between connected devices.. |
| Operator Speed | Displays the current speed of the data transmitted and received over the interface. |
| Admin. Duplex Setting | Displays the administrator's duplex setting. |
| Current Duplex Setting | Displays the interface as either **half duplex**, **full duplex** or **unknown**. |

The **Traffic** field describes the following for the selected access point interface:

| | |
|---|---|
| **Good Octets Sent** | Displays the number of octets (bytes) with no errors sent by the interface. |
| **Good Octets Received** | Displays the number of octets (bytes) with no errors received by the interface. |
| **Good Pkts Sent** | Describes the number of good packets transmitted. |
| **Good Pkts Received** | Describes the number of good packets received. |
| **Mcast Pkts Sent** | Displays the number of multicast packets sent through the selected interface. |
| **Mcast Pkts Received** | Displays the number of multicast packets received through the selected interface. |
| **Ucast Pkts Sent** | Displays the number of unicast packets sent through the selected interface. |
| **Ucast Pkts Received** | Displays the number of unicast packets received through the selected interface. |
| **Bcast Pkts Sent** | Displays the number of broadcast packets sent through the interface. |
| **Bcast Pkts Received** | Displays the number of broadcast packets received through the interface. |
| **Packet Fragments** | Displays the number of packet fragments transmitted or received through the interface. |
| **Jabber Pkts** | Displays the number of packets transmitted through the interface larger than the MTU. |

The **Errors** field displays the following information for the selected access point interface:

| | |
|---|---|
| **Bad Pkts Received** | Displays the number of bad packets received through the interface. |
| **Collisions** | Displays the number of collisions on the interface. |
| **Late Collisions** | A late collision is any collision that occurs after the first 64 octets of data have been sent by the sending client. Late collisions are not normal, and are usually the result of out-of-specification cabling or a malfunctioning device. |
| **Excessive Collisions** | Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point that a single Ethernet network cannot handle it efficiently. |
| **Drop Events** | Displays the number of dropped packets transmitted or received through the interface. |
| **Tx Undersize Pkts** | Displays the number of *undersized* packets transmitted through the interface. |
| **Oversize Pkts** | Displays the number of *oversized* packets transmitted through the interface. |
| **MAC Transmit Error** | Displays the number of transmits that failed because of an internal MAC sublayer error that is not a late collision, excessive collision count, or a carrier sense error. |
| **MAC Receive Error** | Displays the number of received packets failed because of an internal MAC sublayer that is not a late collision, excessive collision count, or a carrier sense error. |
| **Bad CRC** | Displays the CRC error. The *Cyclical Redundancy Check* (CRC) is the 4 byte field at the end of every frame. The receiving station uses it to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of the frame, it's considered a bad CRC. |

The **Receive Errors** field displays the following information about the selected interface:

| | |
|---|---|
| **Rx Frame Errors** | Displays the number of frame errors received at the interface. A frame error occurs when a byte of data is received, but not in the format expected. |
| **Rx Length Errors** | Displays the number of length errors received at the interface. Length errors are generated when the received frame length was less than (or exceeded) the Ethernet standard. |

| | |
|---|---|
| Rx FIFO Errors | Displays the number of FIFO errors received at the interface. *First-in First-Out* queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally. |
| Rx Missed Errors | Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store the incoming packet. |
| Rx Over Errors | Displays the number of overflow errors. An overflow occurs when packet size exceeds the allocated buffer size. |

The Transmit Errors field displays the following:

| | |
|---|---|
| Tx Errors | Displays the number of packets with errors transmitted on the interface. |
| Tx Dropped | Displays the number of transmitted packets dropped from the interface. |
| Tx Aborted Errors | Displays the number of packets aborted on the interface because a *clear-to-send* request was not detected. |
| Tx Carrier Errors | Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or cabling. |
| Tx FIFO Errors | Displays the number of FIFO errors received at the interface. *First-in-First-Out* queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally. |
| Tx Heartbeat Errors | Displays the number of heartbeat errors. This generally indicates a software crash or packets stuck in an endless loop. |
| Tx Window Errors | Displays the number of window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) in the receive window field the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment from the receiving host, it constitutes a window error. |

6 Select **Refresh** to update the statistics counters to their latest value.

### *AP Interface IPv6 Address*

IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

To review IPv6 Address interface statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

The System node expands to display the RF Domains created within the managed network.

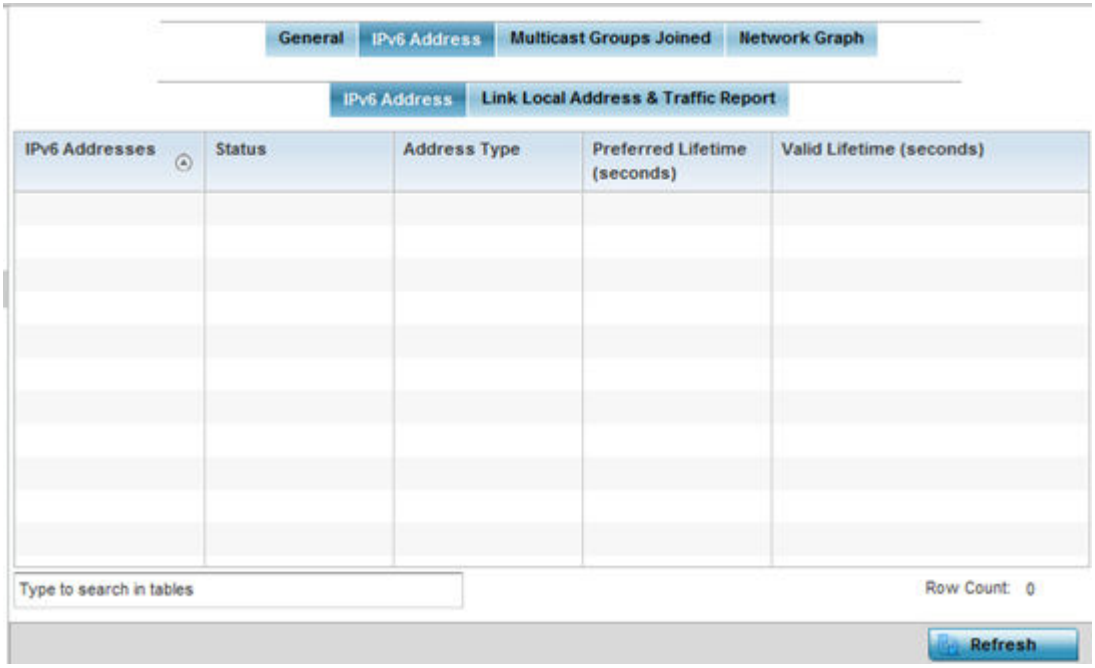
3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Interfaces** menu.

5 Select the **IPv6 Address** tab.

The **Statistics > AP > Interfaces > IPv6 Address > IPv6 Address** screen displays by default in the right-hand pane.




The IPv6 Address table displays the following sections:

| | |
|---|---|
| IPv6 Addresses | Lists the IPv6 formatted addresses currently utilized by the access point in the selected interface. |
| Status | Lists the current utilization status of each IPv6 formatted address currently in use by this access point's selected interface. |
| Address Type | Lists whether the address is *unicast* or *multicast* in its utilization over the selected access point interface. |
| Preferred Lifetime (Seconds) | Lists is the time in seconds (relative to when the packet is sent) the IPv6 formatted addresses remains in a preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime. |
| Valid Lifetime (Seconds) | Displays the time in seconds (relative to when the packet is sent) the IPv6 formatted address remains in a valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime. |

6 Select the **Link Local Address & Traffic Report** tab to assess data traffic and errors discovered in transmitted and received IPv6 formatted data packets.

This screen has the following information:

The Link Local Address table:

| | |
|---|---|
| Address | Lists the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled on, even when one or more routable addresses are assigned. |
| Status | Lists the IPv6 local link address utilization status and its current availability. |

| | |
|---|---|
| Preferred Lifetime (Seconds) | Lists is the time in seconds (relative to when the packet is sent) the local link addresses remains in the preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime. |
| Valid Lifetime (Seconds) | Displays the time in seconds (relative to when the packet is sent) the local link addresses remains in the valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime. |

The **Traffic** table displays the following information:

| | |
|---|---|
| Packets In | Lists the number of IPv6 formatted data packets received on the selected access point interface since the screen was last refreshed. |
| Packets Out | Lists the number of IPv6 formatted data packets transmitted on the selected access point interface since the screen was last refreshed. |
| Bytes In | Displays the number of octets (bytes) with no errors received by the selected interface. |
| Bytes Out | Displays the number of octets (bytes) with no errors sent by the selected interface. |
| Bad Packets Received | Displays the number of bad IPv6 formatted packets received through the interface. |
| Bad CRC | Displays the CRC error. The CRC is the 4 byte field at the end of every frame. The receiving station uses it to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of frame, it is considered as a bad CRC. |
| Collisions | Displays the number of collisions over the selected interface. Excessive collisions occur when the traffic load increases to the point a single Ethernet network cannot handle it efficiently. A late collision is any collision that occurs after the first 64 octets of data have been sent. Late collisions are not normal, and usually the result of out of specification cabling or a malfunctioning device. |

The **Receive Errors** table displays the following information:

| | |
|---|---|
| Receive Length Errors | Displays the number of IPv6 length errors received at the interface. Length errors are generated when the received IPv6 frame length was either less or over the Ethernet standard. |
| Receive Over Errors | Displays the number of IPv6 overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size. |
| Receive Frame Errors | Displays the number of IPv6 frame errors received at the interface. A frame error occurs when data is received, but not in an expected format. |
| Receive FIFO Errors | Displays the number of IPv6 FIFO errors received at the interface. First-in First-out queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority. There is only one queue, and all IPv6 formatted packets are treated equally. An increase in FIFO errors indicates a probable hardware malfunction. |
| Receive Missed Errors | Displays the number of missed IPv6 formatted packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet. |

The Transmit Errors table displays the following information:

| | |
|---|---|
| Transmit Errors | Displays the number of IPv6 formatted data packets with errors transmitted on the interface. |
| Transmit Aborted Errors | Displays the number of IPv6 formatted packets aborted on the interface because a clear-to-send request was not detected. |
| Transmit Carrier Errors | Displays the number of IPv6 formatted carrier errors on the interface. This generally indicates bad Ethernet hardware or bad cabling. |
| Transmit FIFO Errors | Displays the number of IPv6 formatted FIFO errors transmitted at the interface. First-in First-Out queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO uses no priority. There is only one queue, and all packets are treated equally. An increase in the number of FIFO errors indicates a probable hardware malfunction. |
| Transmit Heartbeat Errors | Displays the number of IPv6 formatted heartbeat errors. This generally indicates a software crash, or packets stuck in an endless loop. |
| Transmit Window Errors | Displays the number of IPv6 formatted window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment, it constitutes a window error. |

7 Click **Refresh** to update the statistics counters to their latest value.

### *AP Interface Multicast Groups Joined*

Multicast groups scale to a larger set of destinations by not requiring prior knowledge of who or how many destinations there are. Multicast devices uses their infrastructure efficiently by requiring the source to send a packet only once, even if delivered to a large number of devices. Devices replicate a packet to reach multiple receivers only when necessary.

Access Points are free to join or leave a multicast group at any time. There are no restrictions on the location or members in a multicast group. A host may be a member of more than one multicast group at any given time and does not have to belong to a group to send messages to members of a group.

To view the Access Point's multicast group memberships on the selected interface:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

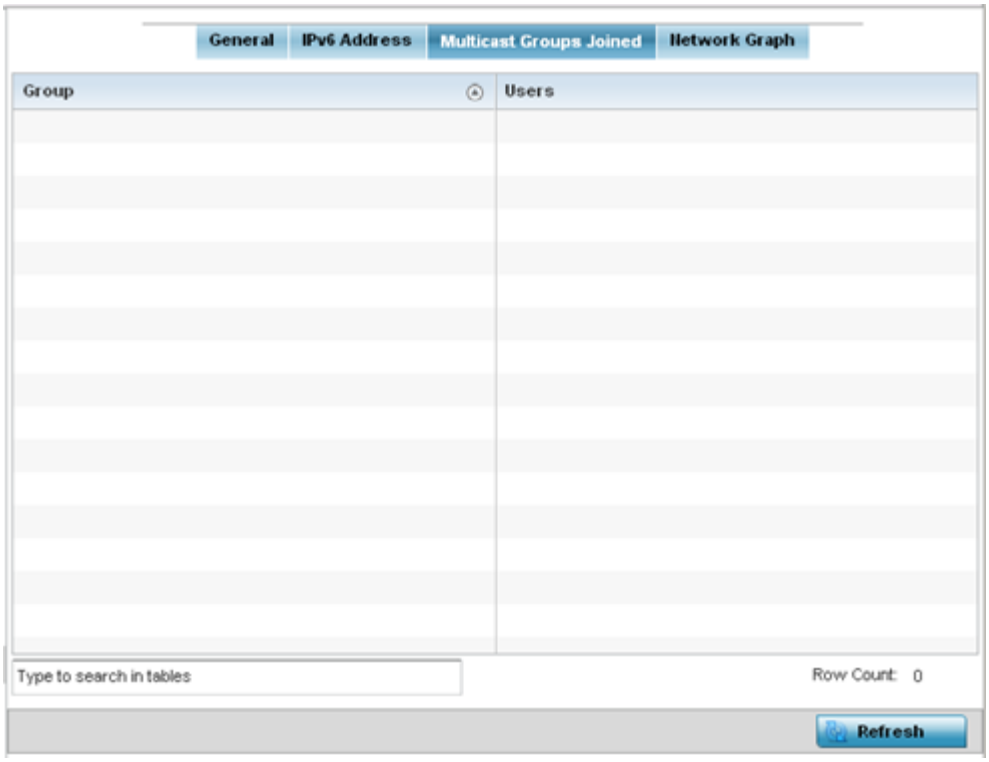
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Interfaces** menu.
5 Select the **Multicast Groups Joined** tab.

The **Statistics > AP > Interfaces > Multicast Groups Joined** displays in the right-hand pane.




This table displays the following information:

| | |
|---|---|
| Group | Lists the name of existing multicast groups whose current members share multicast packets with one another on this selected interface as a means of collective interoperation. |
| Users | Lists the number of devices currently interoperating on this interface in each listed multicast group. Any single device can be a member of more then one group at a time. |

*AP Interface Network Graph*

The Network Graph displays statistics the access point continuously collects for its interfaces. Even when the interface statistics graph is closed, data is still collected. Display the interface statistics graph periodically for assessing the latest interface information. Up to three different stats can be selected and displayed within the graph.

To view a detailed graph for an interface, select an interface and drop it on to the graph. The graph displays Port Statistics as the Y-axis and the Polling Interval as the X-axis. Use the Polling Interval from-down menu to define the increment data is displayed on the graph.

To view the Interface Statistics graph:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

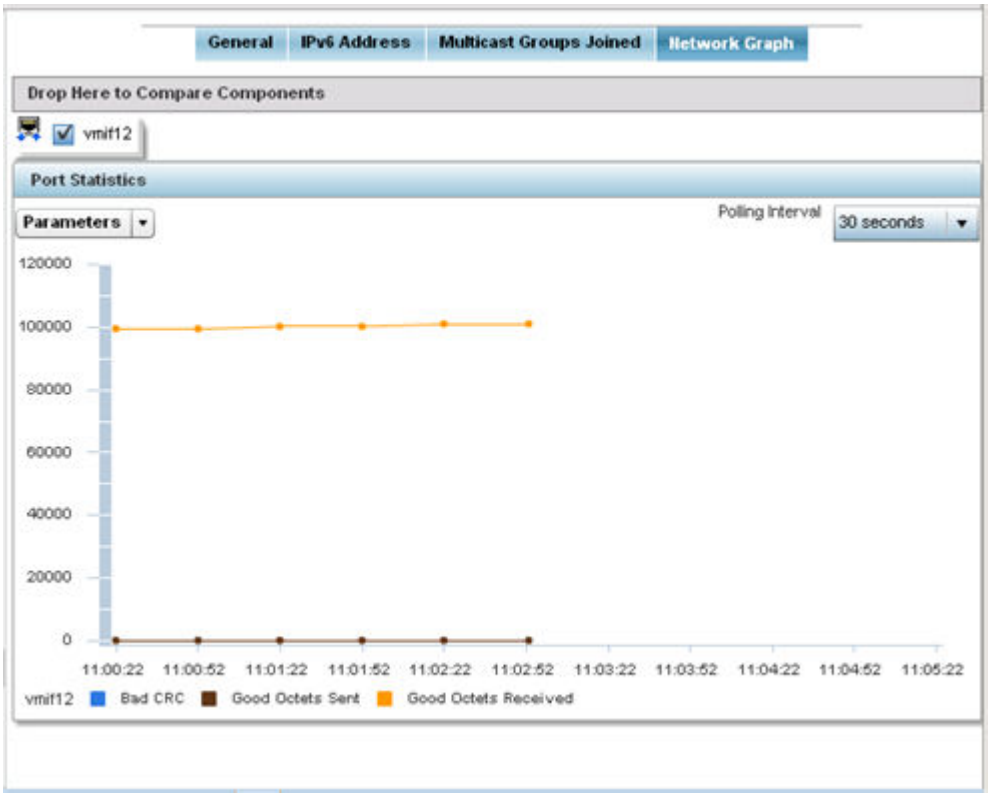
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select the **Interfaces > Network Graph** tab.

The **Statistics > AP > Interfaces > Network Graph** screen displays in the right-hand pane.




5 Use the **Parameters** drop-down menu to specify what is trended in the graph.

## AP RTLS

The RTLS *(real time locationing system)* enables accurate location determination and presence detection capabilities for Wi-Fi-based devices, Wi-Fi-based active RFID tags and passive RFID tags. While the operating system does not support locationing locally, it does report the locationing statistics of both Aeroscout and Ekahau tags.

To review a selected access point's RTLS statistics:

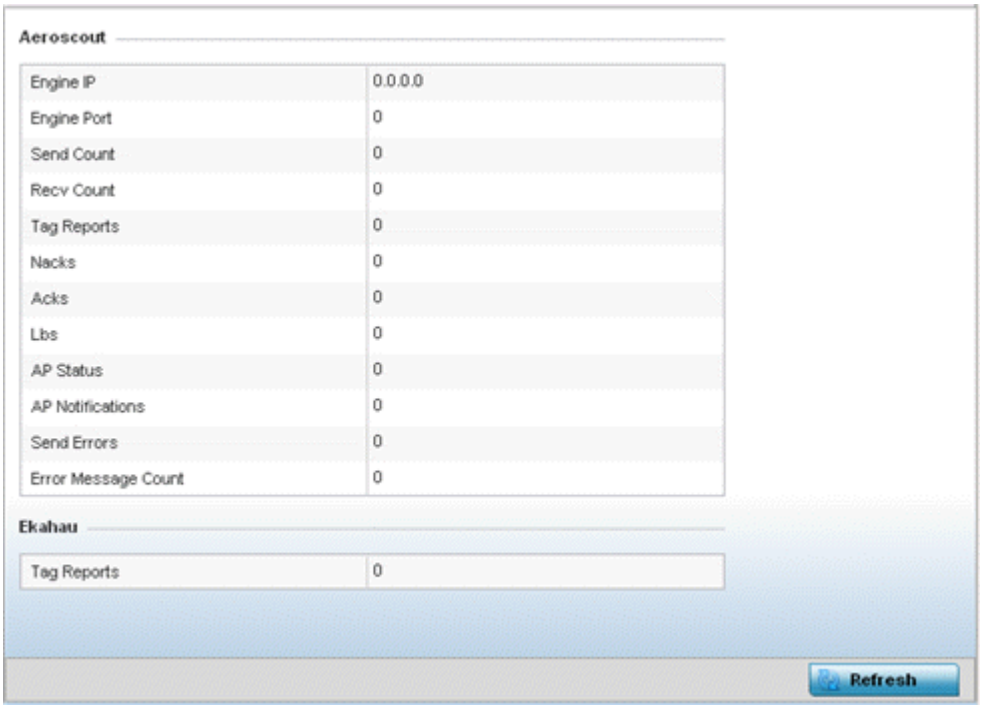
1 Select the Statistics menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select the **RTLS** tab.

The **Statistics > AP > RTLS** screen is displayed.




Review the following *Aeroscout tags* related statistics:

| | |
|---|---|
| Engine IP | Lists the IP address of the Aeroscout locationing engine. |
| Engine Port | Displays the port number of the Aeroscout engine. |
| Send Count | Lists the number location determination packets sent by the locationing engine. |
| Recv Count | Lists the number location determination packets received by the locationing engine. |
| Tag Reports | Displays the number of tag reports received from locationing equipped radio devices supporting RTLS. |
| Nacks | Displays the number of Nack (no acknowledgement) frames received from RTLS supported radio devices providing locationing services. |
| Acks | Displays the number of Ack (acknowledgment) frames received from RTLS supported radio devices providing locationing services. |
| Lbs | Displays the number of LBS *(location based service)* frames received from RTLS supported radio devices providing locationing services. |
| AP Status | Provides the status of peer APs providing locationing assistance. |
| AP Notifications | Displays a count of the number of notifications sent to access points that may be available to provide RTLS support. |
| Send Errors | Lists the number of send errors received by the RTLS initiating access point. |
| Error Message Count | Displays a cumulative count of error messages received from RTLS enabled access point radios. |

Review the following *Ekahau tags* related statistics:

| | |
|---|---|
| Tag Reports | Displays the number of tag reports received from locationing equipped radio devices supporting RTLS. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP PPPoE

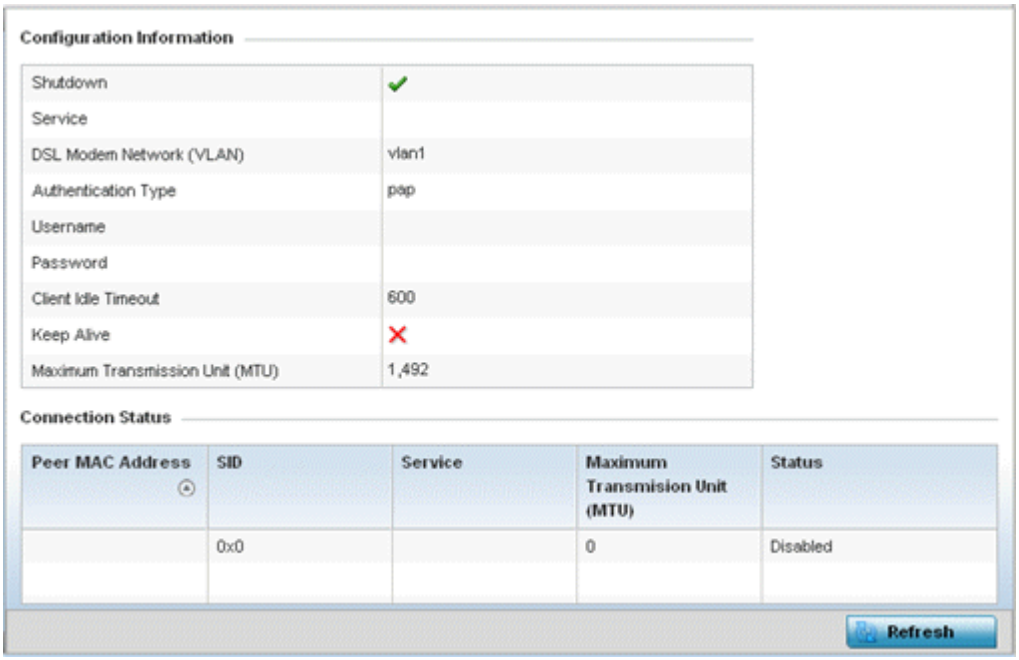
The **PPPoE** statistics screen displays stats derived from an access point's access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables access points to establish a point-to-point connection to an ISP over an existing Ethernet interface.

**Note**
The WiNG 7.1 release does not support PPPoE on AP505 and AP510 model access points. This feature will be supported in future releases.

To review a selected access point's PPPoE statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **PPPoE**.

The **Statistics > AP > PPPoE** screen is displayed.




5 The **Configuration Information** field screen displays the following:

| | |
|---|---|
| Shutdown | Displays whether a high speed client mode point-to-point connection has been enabled using the PPPoE protocol. |
| Service | Lists the 128 character maximum PPPoE client service name provided by the service provider. |
| DSL Modem Network (VLAN) | Displays the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem. |
| Authentication Type | Lists authentication type used by the PPPoE client whose credentials must be shared by its peer access point. Supported authentication options include **None**, **PAP**, **CHAP**, **MSCHAP**, and **MSCHAP-v2**. |
| Username | Displays the 64 character maximum username used for authentication support by the PPPoE client. |
| Password | Displays the 64 character maximum password used for authentication by the PPPoE client. |
| Client Idle Timeout | The access point uses the listed timeout so it does not sit idle waiting for input from the PPPoE client and the server, that may never come. |
| Keep Alive | If a keep alive is utilized, the point-to-point connect to the PPPoE client is continuously maintained and not timed out. |
| Maximum Transmission Unit (MTU) | Displays the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. |

6 Refer to the Connection Status field.

The Connection Status table lists the MAC address, SID, Service information MTU and status of each route destination peer. To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the access point's wired WAN were to fail.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP OSPF

OSPF *(Open Shortest Path First)* is a *link-state* IGP *(interior gateway protocol)*. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

Refer to the following for detailed descriptions of the tabs available within the OSPF statistics screen:

- OSPF Summary
- OSPF Neighbors
- OSPF Area Details
- OSPF Route Statistics

- AP OSPF Interface on page 1022
- OSPF State

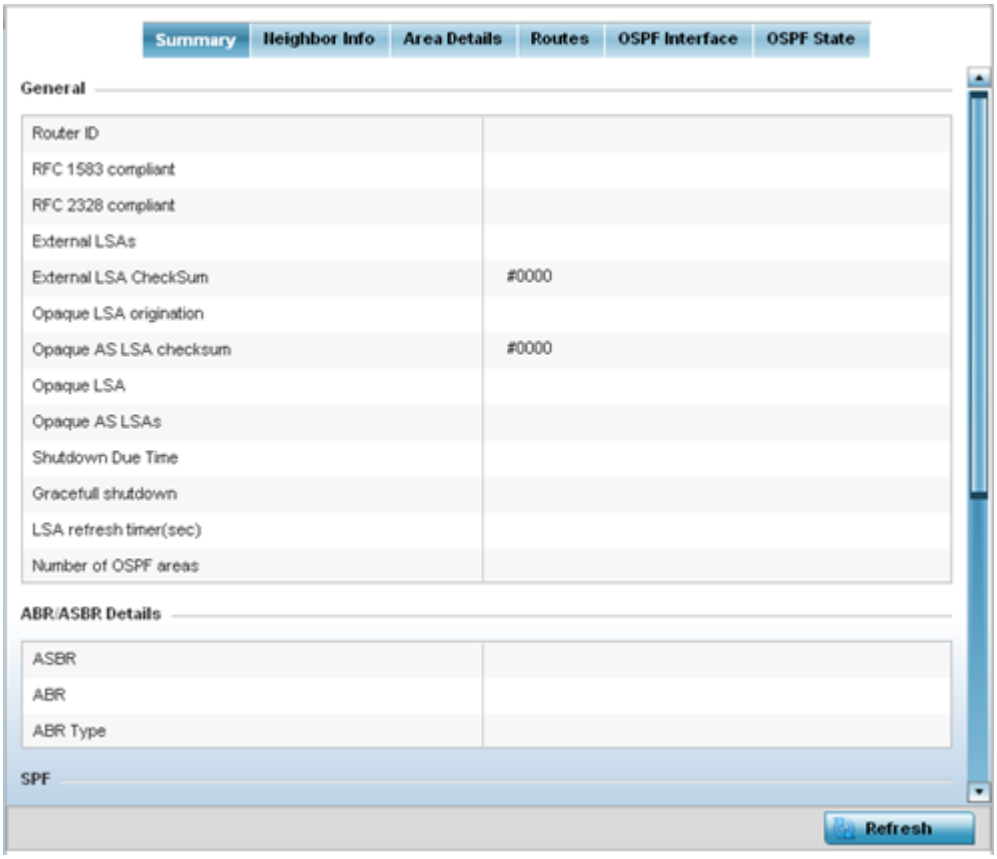
*AP OSPF Summary*

Use the **OSPF Summary** screen to review router ID, area border router, shortest path and stub router connection assignments.

To view OSPF statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **OSPF** menu.

The **Statistics > AP > OSPF > Summary** screen displays by default.




The **Summary** screen describes the following information fields:

| | |
|---|---|
| General | The general field displays the router ID assigned for this OSPF connection, RFC compliance information and LSA data. OSPF version 2 was originally defined within RFC versions 1583 and 2328. The general field displays whether compliance to these RFCs have been satisfied. The OSPF LSA *(Link-State Advertisement)* Throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds. LSA information is provided for both external and opaque LSAs. Opaque LSAs carrying type-length-value elements. These extensions allow OSPF to run completely out of band of the data plane network. This means that it can also be used on non-IP networks, such as optical networks. |
| ABR/ ASBR | Lists ASBR *(Autonomous System Boundary Router)* data relevant to OSPF routing, including the ASBR, ABR and ABR type. An ABR *(Area Border Router)* is a router that connects one or more areas to the main backbone network. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected An ASBR is a router connected to more than one Routing protocol and exchanges routing information with routers in other protocols. ASBRs typically also run an exterior routing protocol (for example, BGP), or use static routes, or both. An ASBR is used to distribute routes received from other, external ASs throughout its own autonomous system. Routers in other areas use ABR as next hop to access external addresses. Then the ABR forwards packets to the ASBR announcing the external addresses. |
| SPF | Refer to the SPF field to assess the status of the SFF *(shortest path forwarding) execution*, *last SPF execution*, *SPF delay*, *SPF due in*, *SPF hold multiplier,SPF hold time*, *SPF maximum hold time* and *SPF timer due flag*. |
| Stub Router | The summary screen displays information relating to stub router advertisements and shutdown and startup times. An OSPF stub router advertisement allows a new router into a network without immediately routing traffic through the new router and allows a graceful shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the OSPF protocol to advertise a maximum or infinite metric to all neighbors. |

5 Select **Refresh** to update the statistics counters to their latest values.

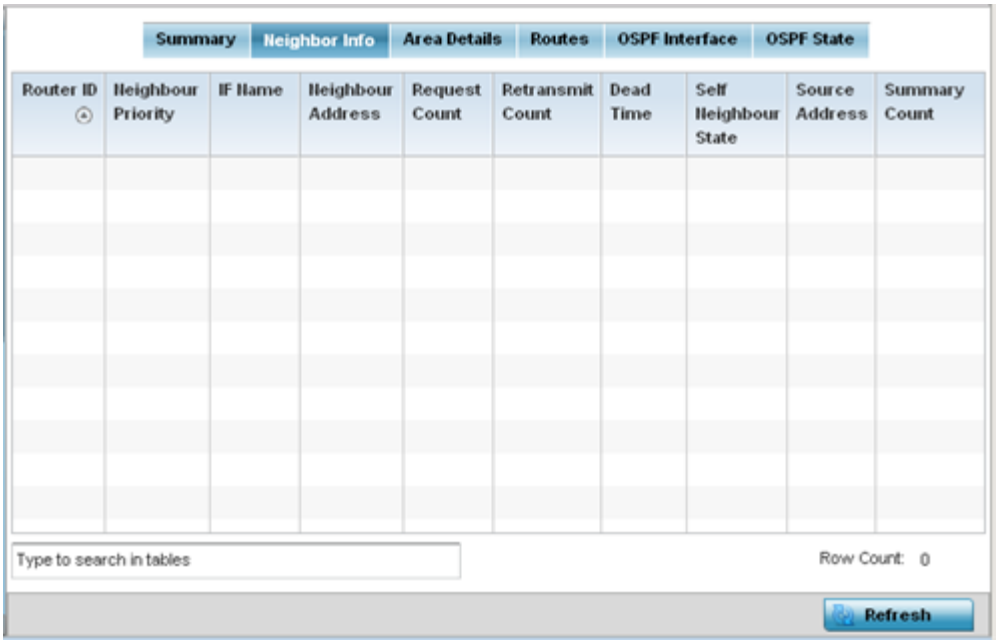
### *AP OSPF Neighbors*

OSPF establishes neighbor relationships to exchange routing updates with other routers. An access point supporting OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a point-to-point link, OSPF knows it is sufficient, and the link stays up. If on a broadcast link, the router waits for election before determining if the link is functional.

To view OSPF neighbor statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **OSPF** menu.
5 Select the **Neighbor Info** tab.

The **Statistics > AP > OSPF > Neighbor Info** screen is displayed.




This screen describes the following:

| | |
|---|---|
| Router ID | Displays the router ID assigned for this OSPF connection. The router is a level three Internet Protocol packet switch. This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network. |
| Neighbor Priority | Displays each listed neighbor's priority in respect to becoming the designated router managing the OSPF connection. The designated router is the router interface elected among all routers on a particular multi-access network segment. |
| IF Name | Lists the name assigned to the router interface used to support connections amongst OSPF enabled neighbors. |
| Neighbor Address | Lists the IP address of the neighbor sharing the router interface with each listed router ID. |
| Request Count | Lists the connection request count (hello packets) to connect to the router interface, discover neighbors and elect a designated router |
| Retransmit Count | Lists the connection retransmission count attempted in order to connect to the router interface, discover neighbors and elect a designated router. A DR *(designated router)* is the router interface elected among all routers on a particular multi-access network segment, generally assumed to be broadcast. |
| Dead Time | Lists the dead time between neighbors in the network topology that are currently utilizing the listed router ID. |
| Self Neighbor State | Displays the self-neighbor status assessment used to discover neighbors and elect a designated router. |
| Source Address | Displays the single source address used by all neighbor routers to obtain topology and connection status. This form of multicasting significantly reduces network load. |
| Summary Count | Routes that originate from other areas are called summary routes. Summary routes are not flooded in a totally stubby or NSSA totally stubby area. |

6 Select **Refresh** to update the statistics counters to their latest values.

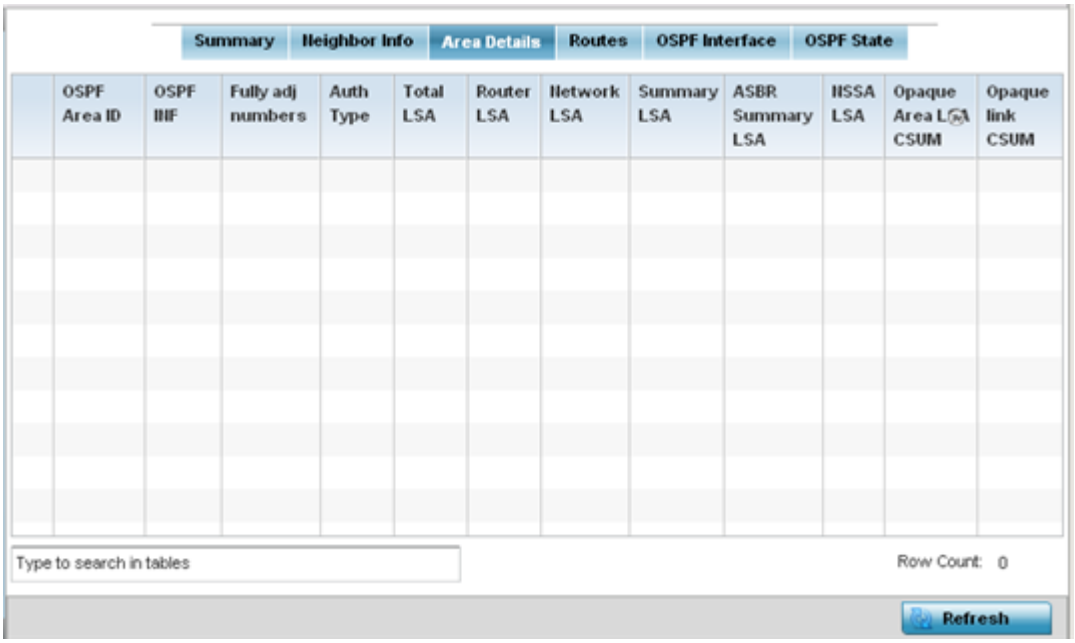
*AP OSPF Area Details*

An OSPF network is subdivided into routing areas (with 32 bit area identifiers) to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network. An OSPF Area contains a set of routers exchanging LSAs with others in the same area. Areas limit LSAs and encourage aggregate routes. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation.

To view OSPF area statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **OSPF** menu.
5 Select the **Area Details** tab.

The **Statistics > AP > OSPF > Area Details** screen is displayed.




The **Area Details** screen describes the following:

| | |
|---|---|
| OSPF Area ID | Displays either the integer (numeric ID) or IP address assigned to the OSPF area as a unique identifier. |
| OSPF INF | Lists the interface ID (virtual interface for dynamic OSPF routes) supporting each listed OSPF area ID. |
| Fully adj numbers | Fully adjusted numbers strip away the effects of other non OSPF and LSA factors and events, leaving only relevant OSPF area network route events counted. |

| | |
|---|---|
| Auth Type | Lists the authentication schemes used to validate the credentials of dynamic route connections and their areas. |
| Total LSA | Lists the LSAs of all entities using the dynamic route (in any direction) in the listed area ID. |
| Router LSA | Lists the LSAs of the router supporting each listed area ID. The router LSA reports active router interfaces, IP addresses and neighbors. |
| Network LSA | Displays which routers are joined together by the designated router on a broadcast segment (e.g., Ethernet). Type 2 LSAs are flooded across their own area only. The link state ID of the type 2 LSA is the IP interface address of the designated route. |
| Summary LSA | The summary LSA is generated by ABR to leak area summary address info into another areas. ABR generates more than one summary LSA for an area if the area addresses cannot be properly aggregated by only one prefix. |
| ASBR Summary LSA | Originated by ABRs when an ASBR is present to let other areas know where the ASBR is. These are supported just like summary LSAs. |
| NSSA LSA | Routers in a NSSA *(Not-so-stubby-area)* do not receive external LSAs from Area Border Routers, but are allowed to send external routing information for redistribution. They use type 7 LSAs to tell the ABRs about these external routes, which the Area Border Router then translates to type 5 external LSAs and floods as normal to the rest of the OSPF network.<br>Redistribution into an NSSA area creates a special type of LSA known as TYPE 7, which can exist only in an NSSA area. An NSSA ASBR generates this LSA, and an NSSA ABR router translates it into type 5 LSA which gets propagated into the OSPF domain. |
| Opaque Area link CSUM | Displays the Type-10 opaque link area checksum with the complete contents of the LSA. Type-10 Opaque LSAs are not flooded beyond the borders of their associated area. |
| Opaque link CSUM | Displays a Type-10 opaque link checksum with the complete contents of the LSA. |

6 Select **Refresh** to update the statistics counters to their latest values.

*AP OSPF Route Statistics*

Refer to the Routes tab to assess the status of OSPF

- AP OSPF Border Routers on page 1018.
- AP OSPF External Routes on page 1019.
- AP OSPF Network Routes on page 1020.
- AP OSPF Router Routes on page 1021.

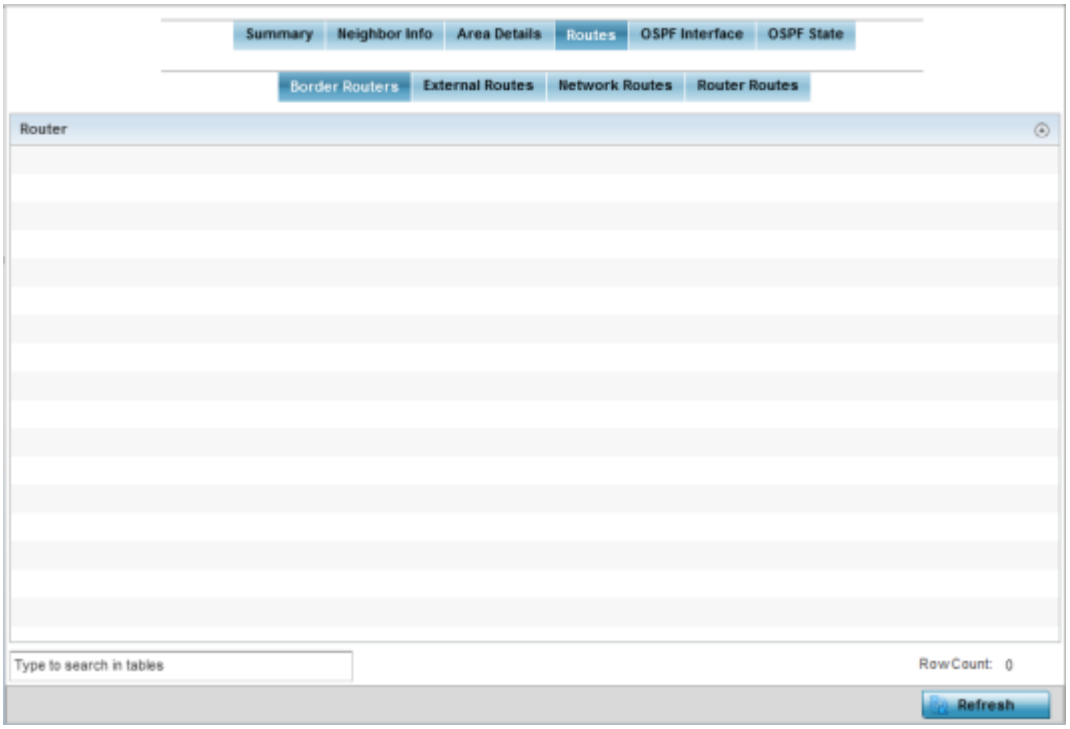
.

### AP OSPF Border Routers

To view OSPF border routers statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **OSPF** menu.
5 Select the **Routes** tab.

The **Statistics > AP > Routes > Border Routers** screen displays by default.




An ABR *(area border router)* connects (links) more than one area. Usually an ABR is used to connect non-backbone areas to the backbone. If OSPF virtual links are used an ABR will also be used to connect the area using the virtual link to another non-backbone area. Border Routers use internal OSPF routing table entries to an ABR or ASBR *(Autonomous System Boundary Router)*. Border routers maintain an LSDB for each area supported. They also participate in the backbone.

6 Select **Refresh** to update the statistics counters to their latest values.

### AP OSPF External Routes

To view OSPF external route statistics:

1 Select the Statistics menu from the Web UI.

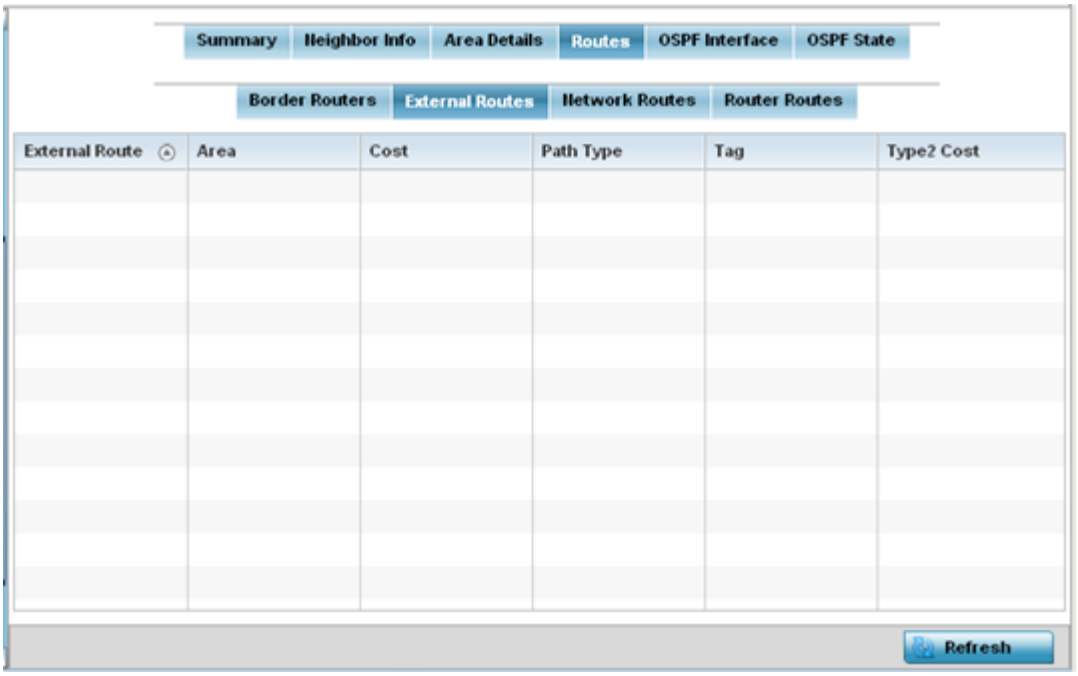
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **OSPF** from the displayed menu.

5 Select the **Routes > External Routes** tab.

The **Statistics > AP > Routes > External Routes** screen is displayed.




External routes are external to area, originate from other routing protocols (or different OSPF processes) and are inserted into OSPF using redistribution. A *stub* area is configured not to carry external routes. Each external route can be tagged by the advertising router, enabling the passing of additional information between routers. Each external route can also be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the autonomous system.

The External route tab displays a list of external routes, the area impacted, cost, path type, tag and type 2 cost. Cost factors may be the distance of a router (round-trip time), network throughput of a link, or link availability and reliability, expressed as simple unit-less numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

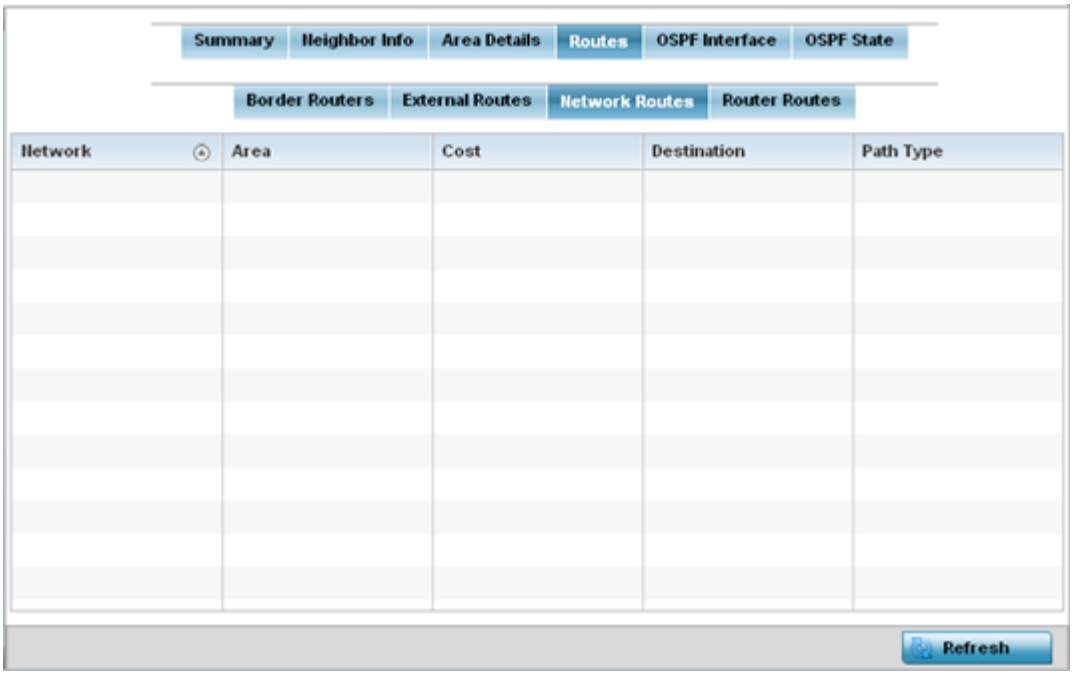
6 Select **Refresh** to update the statistics counters to their latest values.

### AP OSPF Network Routes

To view OSPF network route statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **OSPF** menu.
5 Select the **Routes** tab.
6 Select the **Network Routes** tab.

The **Statistics > AP > Routes > Network Routes** screen is displayed.




Network routes support more than two routers, with the capability of addressing a single physical message to all attached routers (broadcast). Neighboring routers are discovered dynamically using OSPF hello messages. This use of the hello protocol takes advantage of broadcast capability. An OSPF network route makes further use of multicast capabilities, if they exist. Each pair of routers on the network is assumed to communicate directly.

The network tab displays the *network name*, *impacted OSPF area*, *cost*, *destination* and *path type*.

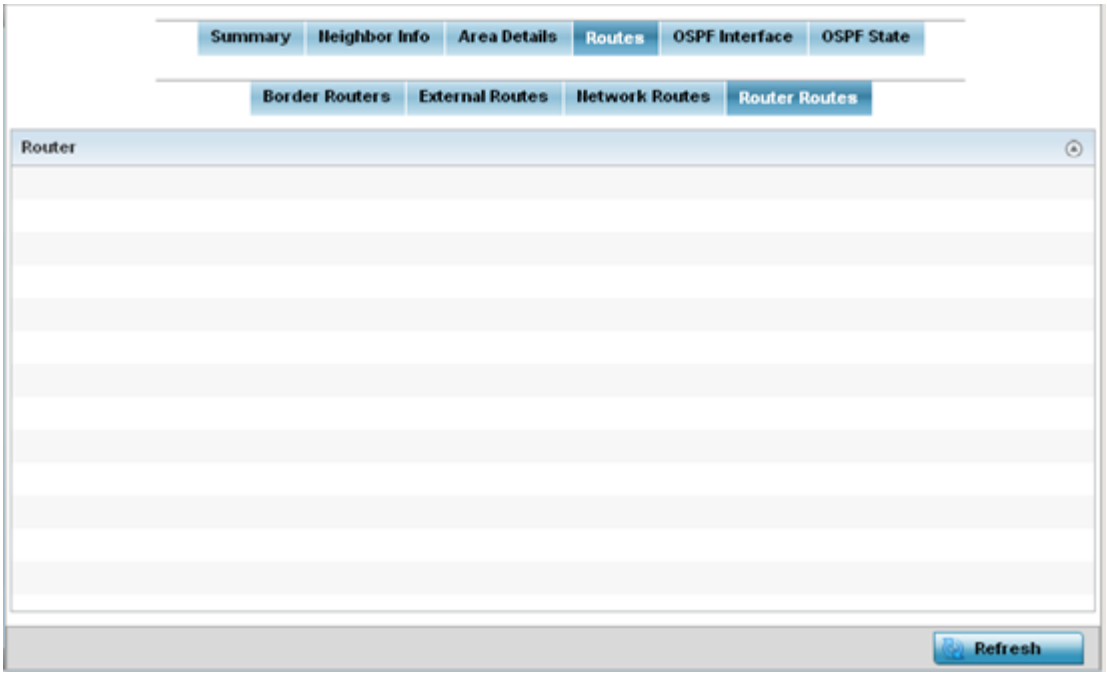
7 Select **Refresh** to update the statistics counters to their latest values.

### AP OSPF Router Routes

To view OSPF router route statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **OSPF** menu.
5 Select the **Routes** tab.
6 Select the **Router Routes** tab.

The **Statistics > AP > Routes > Router Routes** screen is displayed.




An internal (or *router*) route connects to one single OSPF area. All of its interfaces connect to the area in which it is located and does not connect to any other area.

7 Select **Refresh** to update the statistics counters to their latest values.

### *AP OSPF Interface*

An OSPF Interface is the connection between a router and one of its attached networks. An interface has state information associated with it, which is obtained from the underlying lower level protocols and the routing protocol itself. A network interface has associated a single IP address and mask (unless the network is an unnumbered point-to-point network). An interface is sometimes also referred to as a link.

To view OSPF interface statistics:

1 Select the Statistics menu from the Web UI.

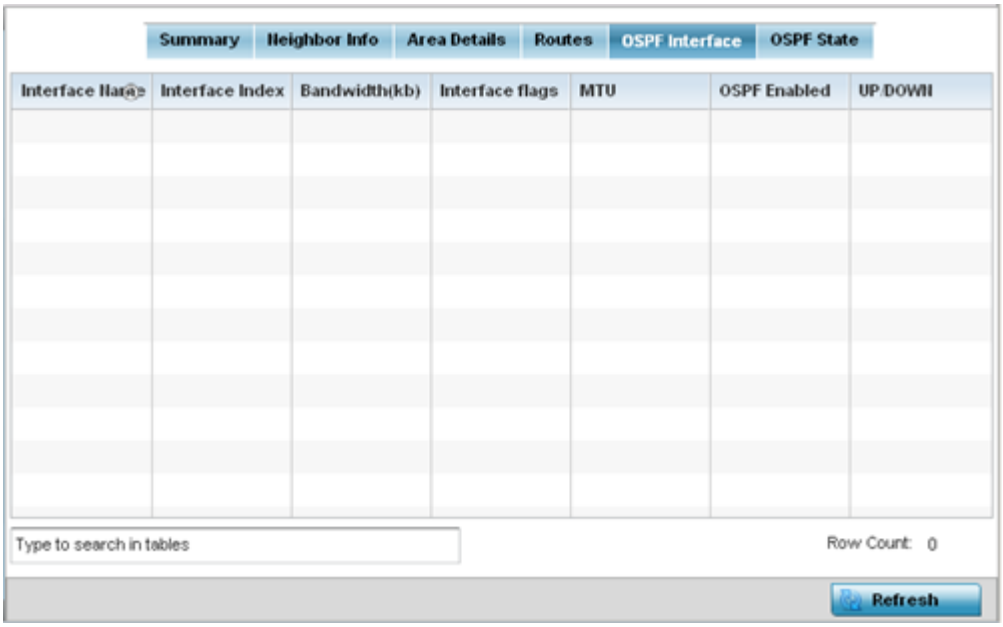
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **OSPF** menu.

5 Select the **OSPF Interface** tab.

The **Statistics > AP > OSPF > OSPF Interface** screen is displayed.




The **OSPF Interface** tab describes the following:

| | |
|---|---|
| **Interface Name** | Displays the IP addresses and mask defined as the virtual interface for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided. |
| **Interface Index** | Lists the numerical index used for the OSPF interface. This interface ID is in the hello packets establishing the OSPF network connection. |
| **Bandwidth** | Lists the OSPF interface bandwidth (in Kbps) in the range of 1 - 10,000,000. |
| **Interface Flag** | Displays the flag used to determine the interface status and how to proceed |
| **MTU** | Lists the OSPF interface MTU size. The MTU is the largest physical packet size (in bytes) a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. |
| **OSPF Enabled** | Lists whether OSPF has been enabled for each listed interface. OSPF is disabled by default. |
| **UP/DOWN** | Displays whether the OSPF interface (the dynamic route) is currently up or down for each listed interface. An OSPF interface is the connection between a router and one of its attached networks. |

6 Select **Refresh** to update the statistics counters to their latest values.

### *AP OSPF State*

An OSPF enabled access point sends hello packets to discover neighbors and elect a designated router for dynamic links. The hello packet includes link ***state*** data maintained on each access point and periodically updated on each OSPF member. The access point tracks link state information to help assess the health of each OSPF dynamic route.

To view OSPF state statistics:

1 Select the **Statistics** menu from the Web UI.

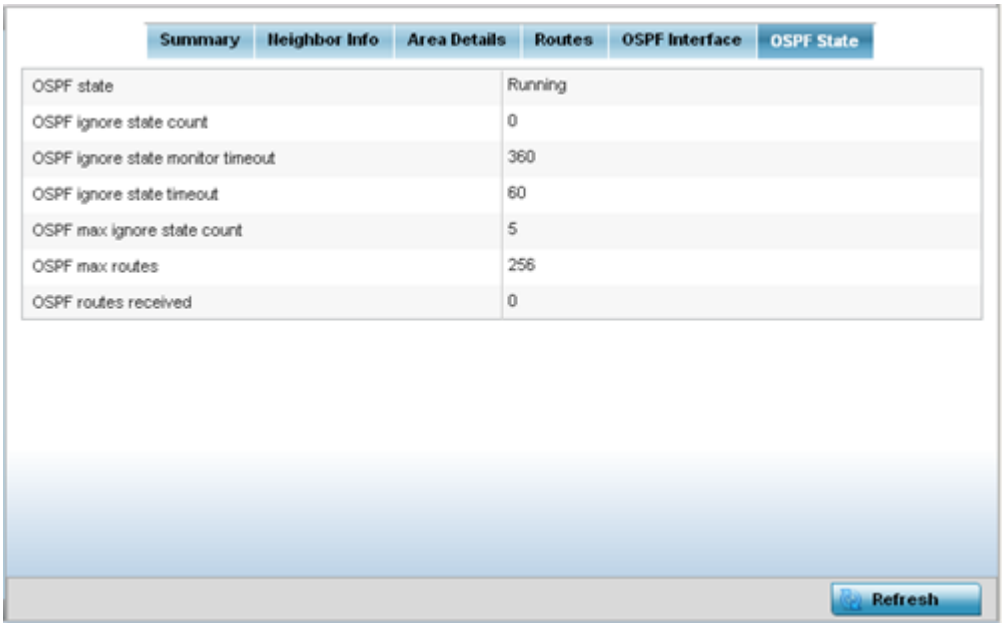
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **OSPF** menu.

5 Select the **OSPF State** tab.

The **Statistics > AP > OSPF > OSPF State** screen is displayed




The **OSPF State**tab describes the following:

| | |
|---|---|
| **OSPF state** | Displays the OSPF link state amongst neighbors within the OSPF topology. Link state information is maintained in a LSDB *(link-state database)* which is a tree image of the entire network topology. Identical copies of the LSDB are periodically updated through flooding on all OSPF supported nodes. Flooding is the part of the OSPF protocol that distributes and synchronizes the link-state database between OSPF routers. |
| **OSPF ignore state count** | Lists the number of times state requests have been ignored between the access point and its peers within this OSPF supported broadcast domain. |
| **OSPF ignore state monitor timeout** | Displays the timeout that, when exceeded, prohibits an access point from detecting changes to the OSPF link state. |
| **OSPF max ignore state count** | Displays whether an OSPF state timeout is being ignored and not utilized in the transmission of state update requests amongst neighbors within the OSPF topology. |
| **OSPF max routes** | States the maximum number of routes negotiated amongst neighbors within the OSPF topology. |
| **OSPF routes received** | Lists the routes received and negotiated amongst neighbors within the OSPF topology. |

6 Select **Refresh** to update the statistics counters to their latest values.

## AP Bluetooth

The AP7602, AP7612, AP7632, AP7662, AP8432 and AP8533 model access points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network.

These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

AP8432 and AP8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone- URL beacons. The access point's Bluetooth radio sends non-connectable, undirected LE *(low-energy)* advertisement packets on a periodic basis. These advertisement packets are short, and they are sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. Portions of the advertising packet are still customizable, however.

**Note**
The WiNG 7.1 release does not support Bluetooth on AP505 and AP510 model access points. This feature will be supported in future releases.

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

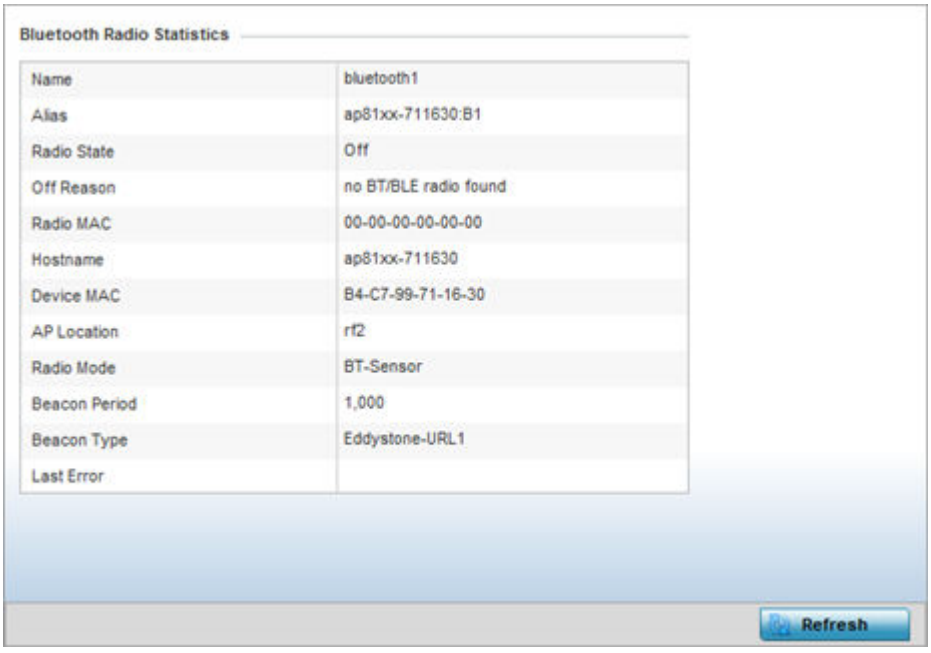
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **Bluetooth**.

The **Statistics → AP → Bluetooth** screen is displayed.




This screen displays the following access point's bluetooth information:

| | |
|---|---|
| Name | Lists the administrator assigned name of the access point's Bluetooth radio. |
| Alias | If an alias has been defined for the AP it is listed here. The alias value is expressed in the form of <hostname>: B<bluetooth_radio_number>. If the administrator has defined a hostname for the AP, it is used in place of the AP's default hostname. |
| Radio State | Displays the current operational state (*On*/*Off*) of the Bluetooth radio. |
| Off Reason | If the Bluetooth radio is *offline*, this field states the reason. |
| Radio MAC | Lists the Bluetooth radio's factory-encoded MAC address serving as this device's hardware identifier on the network. |
| Hostname | Lists the AP's hostname as its network identifier. |
| Device MAC | Lists the AP's factory-encoded MAC address serving as this device's hardware identifier on the network. |
| AP Location | Lists the AP's administrator-assigned deployment location. |
| Radio Mode | Lists an Access Point's Bluetooth radio functional mode as either **`btsensor`** or **`le-beacon`**. |
| Beacon Period | Lists the Bluetooth radio's beacon transmission period from 100 -10,000 milliseconds. |
| Beacon Type | Lists the type of beacon currently configured. |
| Last Error | Lists descriptive text on any error that is preventing the Bluetooth radio from operating. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

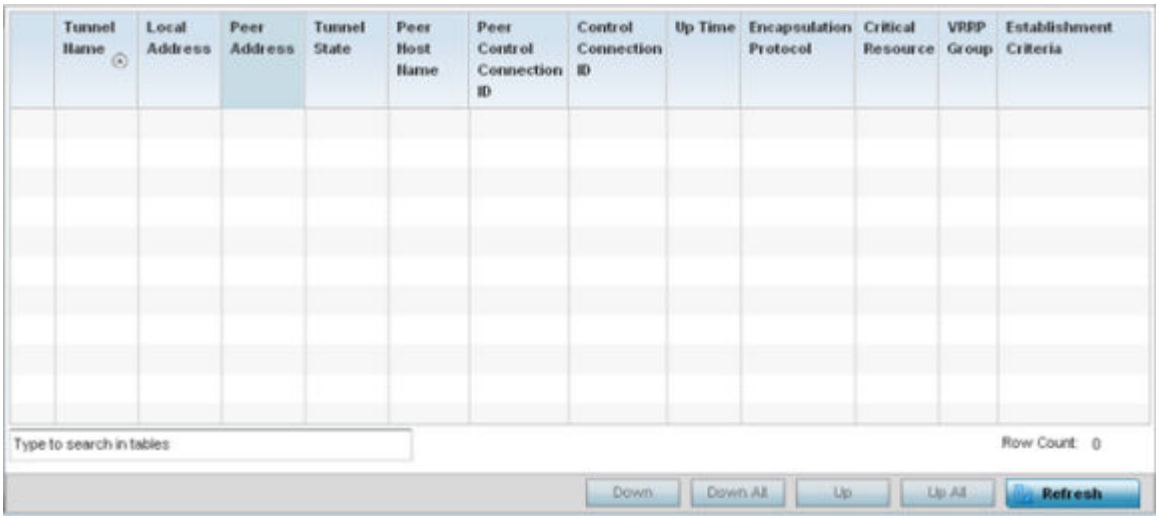
## AP L2TPv3 Tunnels

Access points use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables an access point to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WiNG devices and other vendor devices supporting the L2TP V3 protocol.

To review a selected access point's L2TPv3 statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Select **L2TPv3 Tunnels** from the menu.

The **Statistics → AP → L2TPv3 Tunnels** screen is displayed.




This screen displays the following:

| | |
|---|---|
| Tunnel Name | Displays the name of each listed L2TPv3 tunnel assigned upon creation. Each listed tunnel name can be selected as a link to display session data specific to that tunnel. The Sessions screen displays cookie size information as well as psuedowire information specific to the selected tunnel. Data is also available to define whether the tunnel is a trunk session and whether tagged VLANs are used. The number of transmitted, received and dropped packets also display to provide a throughput assessment of the tunnel connection. Each listed session name can also be selected as a link to display VLAN information specific to that session. The VLAN Details screen lists those VLANs used an access point interface in L2TP tunnel establishment. |
| Local Address | Lists the IP address assigned as the local tunnel end point address, not the tunnel interface's IP address. This IP is used as the tunnel source IP address. If a local address is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. |
| Peer Address | Lists the IP address of the L2TP tunnel peer establishing the tunnel connection. |
| Tunnel State | States whether the tunnel is Idle (not utilized by peers) or is currently active. |
| Peer Host Name | Lists the assigned peer hostname used as matching criteria in the tunnel establishment process. |
| Peer Control Connection ID | Displays the numeric identifier for the tunnel session. This is the peer pseudowire ID for the session. This source and destination IDs are exchanged in session establishment messages with the L2TP peer. |
| Control Connection ID | Displays the router ID(s) sent in tunnel establishment messages with a potential peer device. |
| Up Time | Lists the amount of time the L2TP connection has remained established amongst peers sharing the L2TPv3 tunnel connection. The Up Time is displayed in a Days: Hours: Minutes: Seconds: format. If D:0 H:0 M:0 S:0 is displayed, the tunnel connection is not currently established. |
| Encapsulation Protocol | Displays either IP or UDP as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes. Tunneling is also called encapsulation. Tunneling works by encapsulating a network protocol within packets carried by the second network. |

| | |
|---|---|
| Critical Resource | Lists critical resources for this tunnel. Critical resources are device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the network. These device addresses are pinged regularly by access points. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. |
| VRRP Group | Lists a VRRP group ID (if utilized). A VRRP group is only enabled when the establishment criteria is set to *vrrp-master*. A VRRP master responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. |
| Establishment Criteria | Displays the tunnel establishment criteria for this tunnel. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host. |

5 Select **Refresh** to update the screen's statistics counters to their latest value.

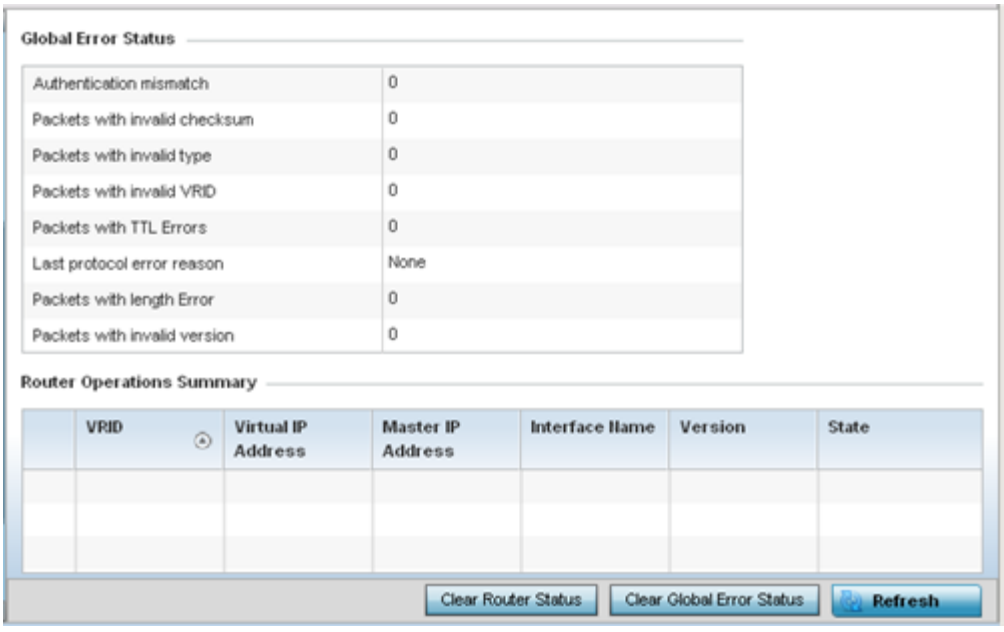
## AP VRRP

The **VRRP** screen displays VRRP *(Virtual Router Redundancy Protocol)* configuration statistics supporting router redundancy in a wireless network requiring high availability.

To review a selected access point's VRRP statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **VRRP**.

The **Statistics > AP > L2TPv3 Tunnels** screen is displayed.




5 Refer to the **Global Error Status** field to review the various sources of packet errors logged during the implementation of the virtual route.

Errors include the mismatch of authentication credentials, invalid packet checksums, invalid packet types, invalid virtual route IDs, TTL errors, packet length errors and invalid (non matching) VRRP versions.

6 Refer to the Router Operations Summary for the following status:

| | |
|---|---|
| VRID | Lists a numerical index (1 - 254) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for. |
| Virtual IP Address | Lists the virtual interface IP address used as the redundant gateway address for the virtual route. |
| Master IP Address | Displays the IP address of the elected VRRP master. A VRRP master (once elected) responds to ARP requests, forwards packets with a destination link layer MAC address equal to the virtual router MAC address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. |
| Interface Name | Displays the interfaces selected on the access point to supply VRRP redundancy failover support. |
| Version | Display VRRP version 3 (RFC 5798) or 2 (RFC 3768) as selected to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. |
| State | Displays the current state of each listed virtual router ID. |

7 Select **Clear Router Status** to clear the Router Operations Summary table to zero and begin new data collections.

8 Select **Clear Global Error Status** to clear the Global Error Status table values to zero and begin new data collections.

9 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Critical Resources

The Critical Resources screen displays device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the access point managed network. Critical resources are pinged regularly by the access point. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. Each device's VLAN, ping mode and state is displayed for the administrator.

To review a selected access point's critical resource statistics:

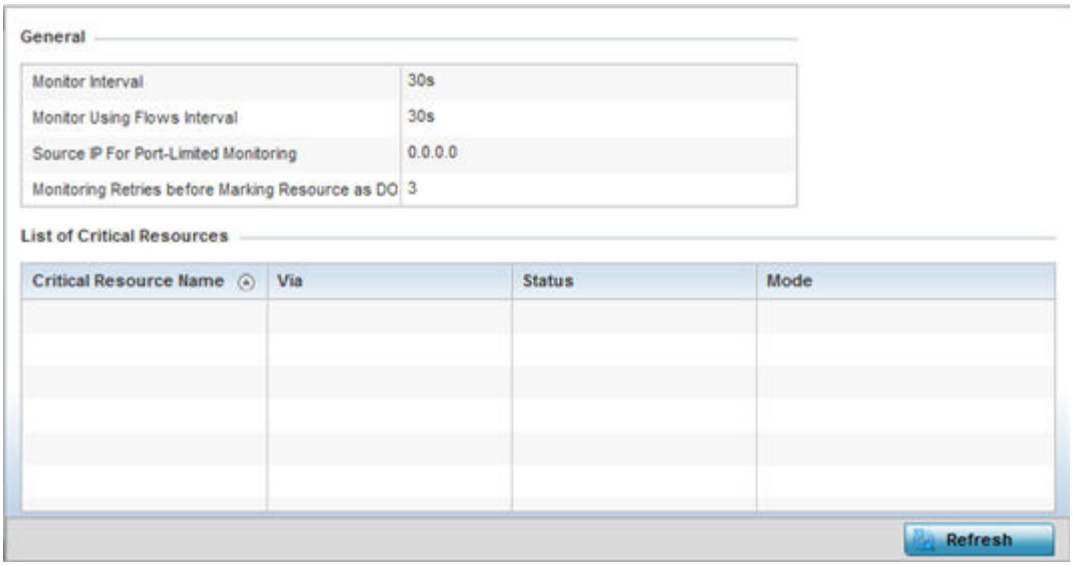
1 Select the Statistics menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Critical Resource** from the left-hand side of the UI.

The **Statistics > AP > Critical Resource** screen is displayed in the right-hand pane.




Refer to the General field to assess the Monitor Interval and Monitor Using Flows Interval used to poll for updates from the critical resource IP listed for Source IP For Port Limited Monitoring. Monitoring Retries before Marking resource as DOWN are the number of retry connection attempts permitted before this listed resource is defined as down (offline).

Refer to the following List of Critical Resources stats:

| | |
|---|---|
| Critical Resource Name | Lists the name of the critical resource monitored by the access point. Critical resources are device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the network. These device addresses are pinged regularly by access points. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. |
| Via | Lists the VLAN used by the critical resource as a virtual interface. the VLAN displays as a link than can be selected to list configuration and network address information in greater detail. |
| Status | Defines the operational state of each listed critical resource VLAN interface (**Up** or **Down**). |
| Error Reason | Provides an error status as to why the critical resource is not available over its designated VLAN. |
| Mode | Defines the operational state of each listed critical resource (up or down). |

5 Select **Refresh** to update the statistics counters to their latest values.

## AP LDAP Agent Status

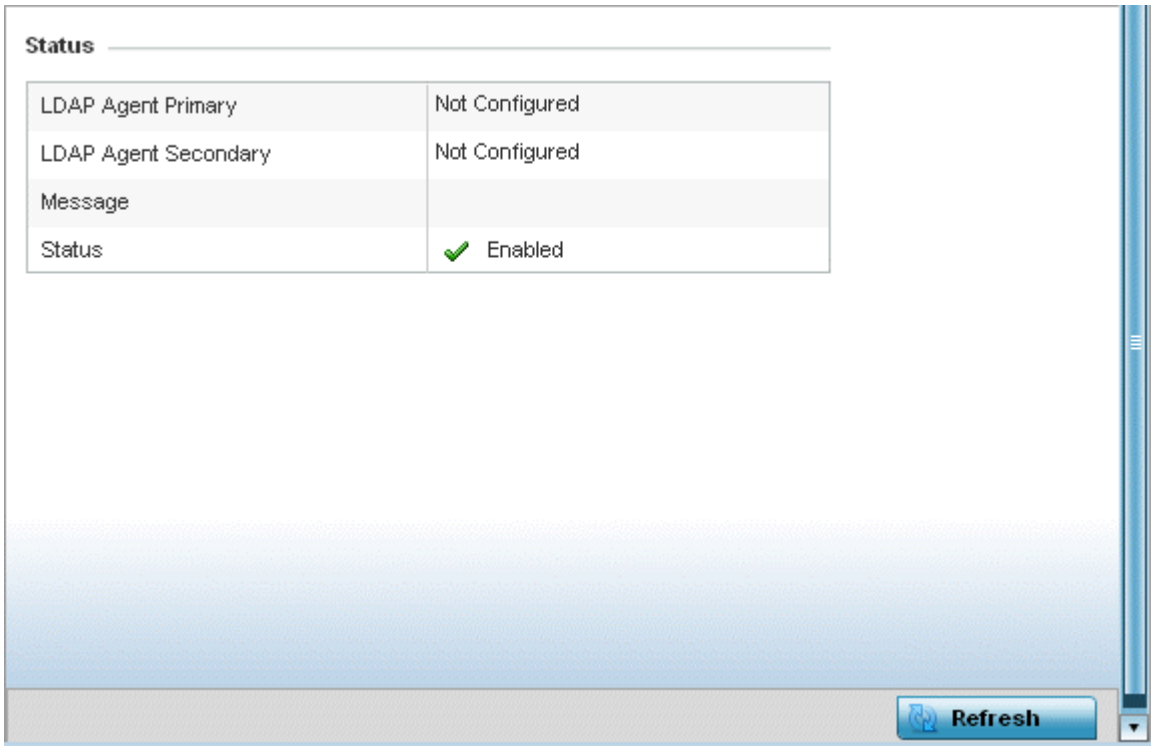
When LDAP has been specified as an external resource (as opposed to local access point RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary and secondary external resources) can be defined as external resources for PEAP-MS-CHAP v2 authentication requests.

For more information on setting LDAP agents as part of the RADIUS server policy, see Configuring RADIUS Server Policy on page 833.

To view access point LDAP agent statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **LDAP Agent Status** from the left-hand side of the UI.

The **Statistics → AP → LDAP Agent Status** screen is displayed in the right-hand pane.




The LDAP Agent Status screen displays the following:

| | |
|---|---|
| LDAP Agent Primary | Lists the primary IP address of a remote LDAP server resource used by the controller or service platform to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the first resource for authentication requests. |
| LDAP Agent Secondary | Lists the secondary IP address of a remote LDAP server resource used by the controller or service platform to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the second resource for authentication requests. |
| Message | Displays any system message generated in the controller or service platform's connection with the primary or secondary LDAP agent. If there's a problem with the username and password used to connection to the LDAP agent it would be listed here. |
| Status | Displays whether the controller or service platform has successfully joined the remote LDAP server domain designated to externally validate PEAP-MS-CHAP v2 authentication requests. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP MiNT Links

Wireless controllers and APs use the MiNT protocol as the primary means of device discovery and communication for AP adoption and management. MiNT provides a mechanism to discover neighbor devices in the network, and exchange packets between devices regardless of how these devices are connected (L2 or L3).

MiNT Links are automatically created between controllers and APs during adoption using MLCP *(MiNT Link Creation Protocol)*. They can also be manually created between a controller and AP (or) between two APs. MiNT links are manually created between controllers while configuring a cluster.

Level 2 (or) remote MiNT links are controller aware links, and requires IP network for communication. This level 2 MiNT links at access points are intended for remote Adaptive AP deployment and management from NOC. With Level2 MiNT links, access points are only aware of the controllers and not about other APs. Level 2 MiNT links also provide partitioning, between APs deployed at various remote sites.

To view access Mint link statistics:

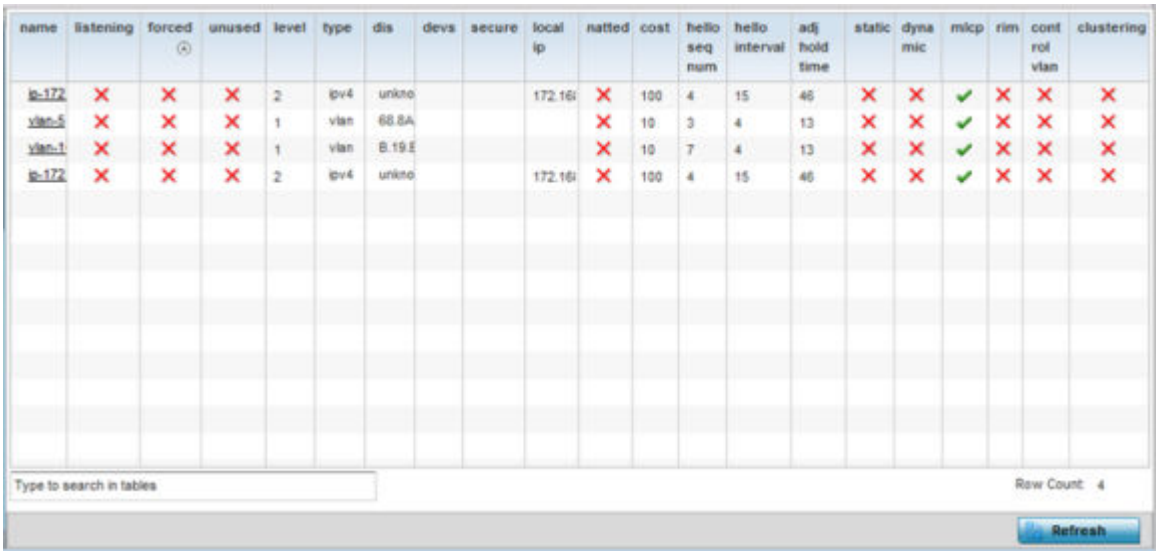
1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

  The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points.

  The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Mint Links** from the left-hand side of the UI.

The **Statistics > AP > Mint Links** screen is displayed in the right-hand pane.



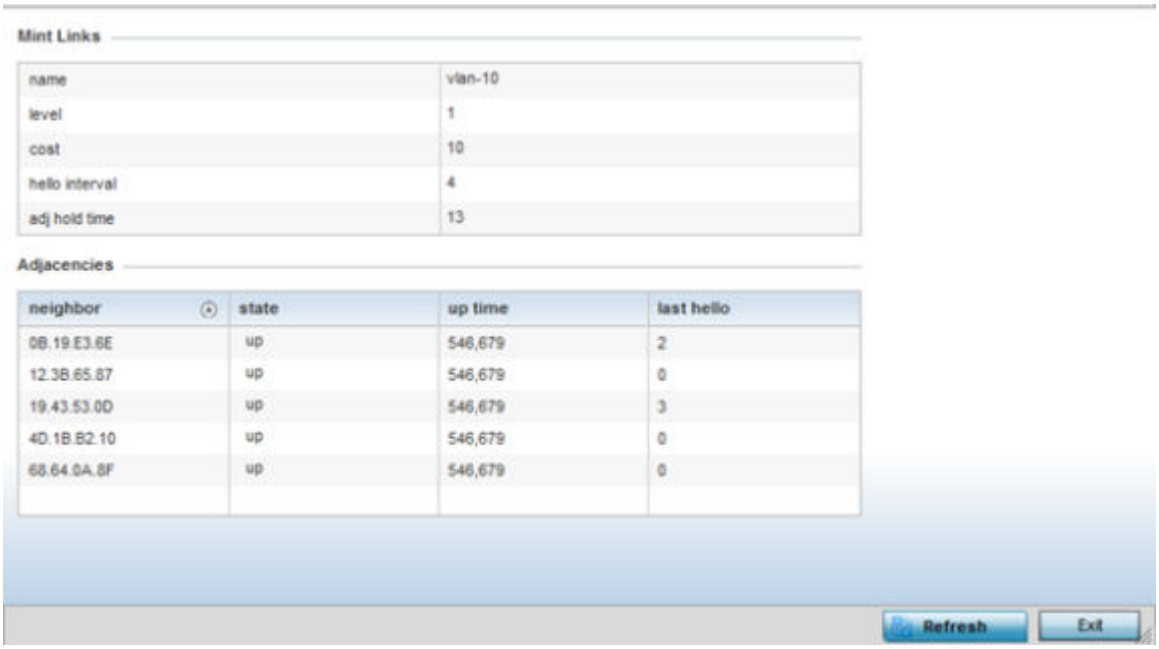

The Mint Links screen lists the name of the impacted VLAN or link in the form of a link that can be selected to display more granular information about that VLAN. A green check mark or a red X defines whether the listed VLAN is listening to traffic, forced to stay up or unused with the Mint link. The level column specifies whether the listed Mint link is traditional switching link (level 2) or a routing link (level 3). The type column defines whether the listed Mint link is a VLAN or an IPv4 or IPv6 type network address. The dis column lists how each link was discovered.

Refer to the secure column to assess whether the listed links are isolated between peers. The local ip column lists the IP address assigned as the link's end point address, not the interface's IP address. The natted column lists whether the link is NAT enabled or disabled for modifying network address information in IP packet headers in transit. The cost column defines the cost for a packet to travel from its originating port to its end point destination.

The hello seq number and hello interval columns define the interval between hello keep alive messages between link end points. While the adj hold time sets the time after the last hello packet when the connected between end points is defined as lost.

The static and dynamic link columns state whether each listed link is static route using a manually configured route entry, or a dynamic route characterized by its destination. The rim column defines whether the listed link is managed remotely. The control vlan column states whether the listed link has enabled as a control VLAN. Lastly, the clustering column states whether listed link members discover and establish connections to other peers and provide self-healing in the event of cluster member failure.

5 If needed, select a **Mint link** from the **name** column to display more granular information for that link.




The first table lists the Mint link's name and level specifying whether the Mint link is traditional switching link (level 2) or a routing link (level 3). The cost defines the cost for a packet to travel from its originating port to its end point destination. The hello interval lists the time between hello keep alive messages between link end points. The adj hold time sets the time after the last hello packet when the connected between end points is defined as lost.

The Adjacencies table lists neighbor devices by their hardware identifiers and operational state to help determine their availability as Mint link end points and peers. The up time lists the selected link's detection on the network and the last hello lists when the last hello message was exchanged.

6 Periodically, select **Refresh** to update the screen's data counters to their latest values.

## AP Guest Users

A captive portal is an access policy for providing guests temporary and restrictive access to the wireless network. A captive portal configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Captive portals can have their access durations set by an administrator to either provide temporary access to the access point managed network or provide access without limitations.

For information on setting captive portal duration and authentication settings, refer to Captive Portal Policies on page 785.

To view an access point's connected guest user client statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

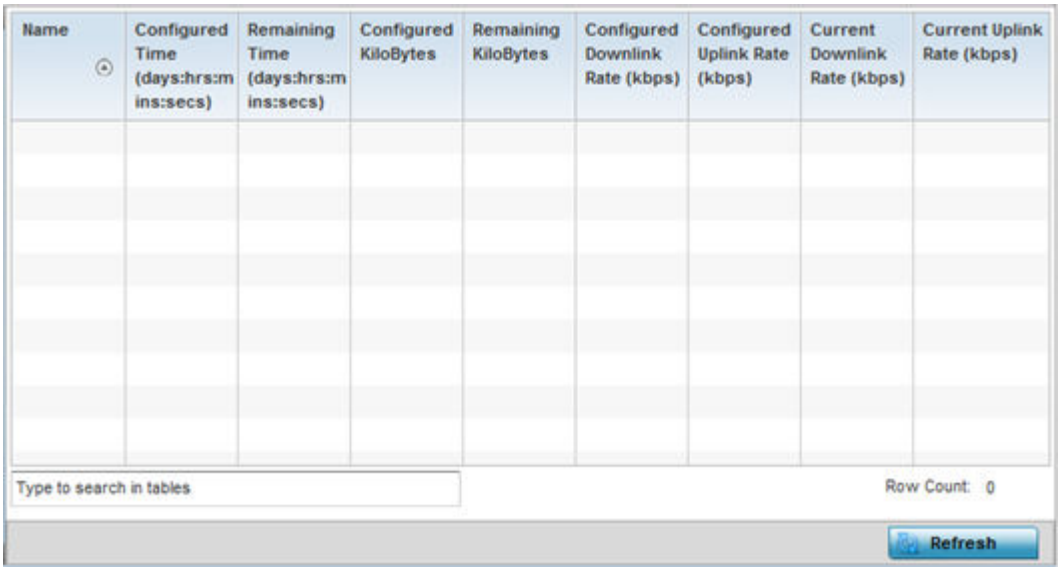
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **Guest User** from the left-hand side of the UI.

The **Statistics > AP > Guest User** screen displays.




This screen describes the following:

| | |
|---|---|
| Name | Lists the administrator assigned name of the client utilizing the access point for guest access to the wireless network. |
| Configured Time (days:hrs:mins:secs) | Displays the restricted permissions each listed client was initially configured for their captive portal guest user session with this managing access point. |
| Remaining Time (days:hrs:mins:secs) | Displays the time each listed client has remaining in their captive portal guest user session with this managing access point. |
| Configured Kilobytes | Lists the maximum configured bandwidth consumable by the listed guest user (in kilobytes). |
| Remaining Kilobytes | Lists the remaining bandwidth available to the listed guest user (in kilobytes). This is the difference between the configured (maximum) bandwidth and the user's current utilization. |
| Configured Downlink Rate (kbps) | Specifies the download speed configured for the listed guest user. When bandwidth is available, the user can download data at the specified rate (in kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the defined reduced downlink rate. For more information, refer to Defining User Pools on page 828. |
| Configured Uplink Rate (kbps) | Specifies the upload speed dedicated to the listed guest user. When bandwidth is available, the user is able to upload data at the specified rate (in kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the reduced uplink rate. For more information, refer to Defining User Pools on page 828. |

| | |
|---|---|
| Current Downlink Rate (Kbps) | Lists the listed guest user's current downlink rate in kbps. Use this information to assess whether this user's configured downlink rate is adequate for their session requirements and whether their reduced downlink rate need adjustment if the configured downlink rate is exceeded. For more information, refer to Defining User Pools on page 828. |
| Current Uplink Rate (Kbps) | Lists the listed guest user's current uplink rate in kbps. Use this information to assess whether this user's configured uplink rate is adequate for their session requirements and whether their reduced uplink rate need adjustment if the configured uplink rate is exceeded. For more information, refer toDefining User Pools on page 828 . |

5 Click **Refresh** to update the statistics counters to their latest values.

## AP GRE Tunnel

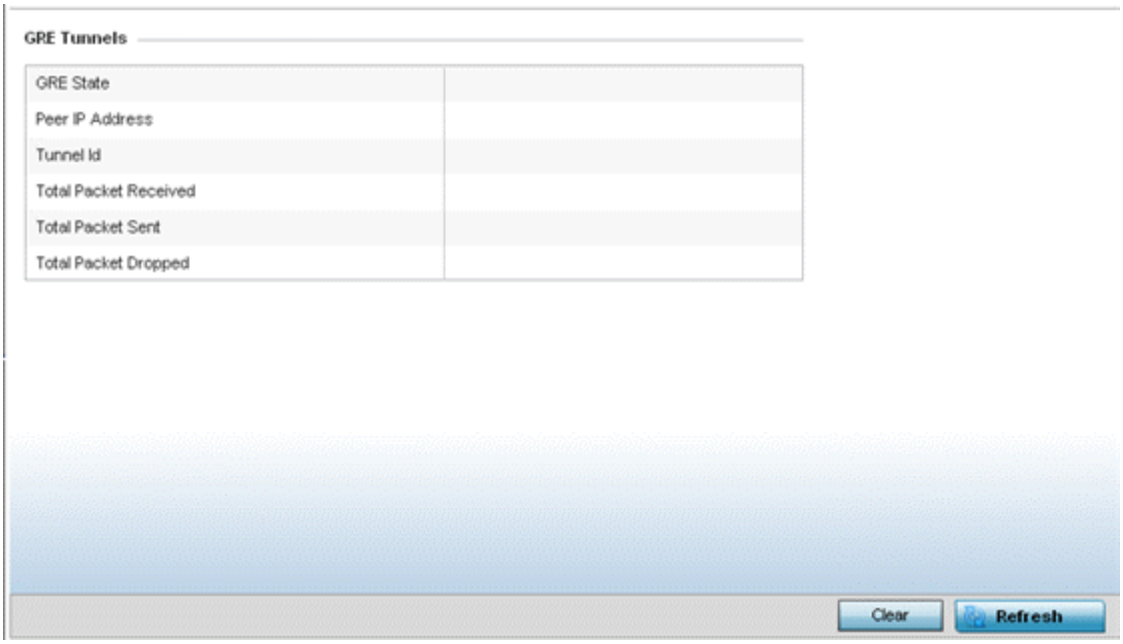
*Generic Routing Encapsulation* (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

Use the GRE Tunnel screen to view information on the traffic flow in a *Generic Routing Encapsulation* (GRE) tunnel.

To view the access point's GRE Tunnel statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **GRE Tunnel**.

The **Statistics > AP > GRE Tunnels** screen displays in the right-hand pane.




This screen describes the following:

| | |
|---|---|
| GRE State | Displays the current operational state of the GRE tunnel. |
| Peer IP Address | Displays the IP address of the peer device on the remote end of the GRE tunnel. |
| Tunnel ID | Displays the session ID of an established GRE tunnel. This ID is only viable while the tunnel is operational and does not carry to subsequent sessions. |
| Total Packets Received | Displays the total number of packets received from a peer at the remote end of the GRE tunnel. |
| Total Packets Sent | Displays the total number of packets sent from this controller or service platform to a peer at the remote end of the GRE tunnel. |
| Total Packets Dropped | Lists the number of packets dropped from tunneled exchanges between this controller or service platform and a peer at the remote end of the VPN tunnel |

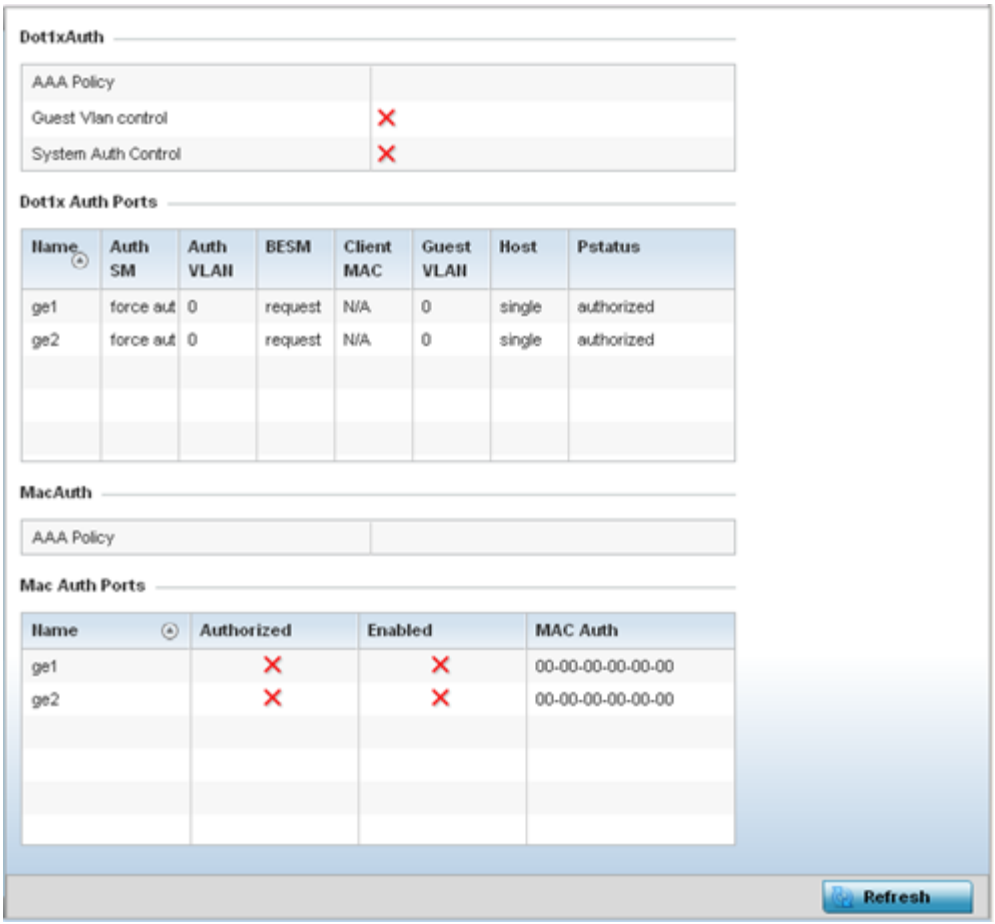
## AP Dot 1X

*Dot1x* (or 802.1x) is an IEEE standard for network authentication. Devices supporting Dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a Dot1x network, a device automatically connects and authenticates without needing to manually login.

To view the Dot1x statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **Dot1x** from the left-hand side of the UI.

The **Statistics > AP > Dot1X** screen is displayed.




Refer to the following **Dot1xAuth** statistics:

| | |
|---|---|
| AAA Policy | Lists the AAA policy currently being utilized for authenticating user requests. |
| Guest Vlan Control | Lists whether guest VLAN control has been allowed (or enabled). This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled. A green checkmark designates guest VLAN control as enabled. A red X defines guest VLAN control as disabled. |
| System Auth Control | Lists whether Dot1x authorization is globally enabled for the controller or service platform. A green checkmark designates Dot1x authorization globally enabled. A red X defines Dot1x as globally disabled. |

Review the following **Dot1x Auth Ports** utilization information:

| | |
|---|---|
| Name | Lists the controller or service platform GE ports subject to automatic connection and authentication using Dot1x. |
| Auth SM | Lists whether Dot1x authentication is forced over the listed port. |
| Auth VLAN | Lists the numeric VLAN ID used as a virtual interface for authentication requests over the listed port. |
| BESM | Lists whether an authentication request is pending on the listed port. |
| Client MAC | Lists the MAC address of requesting clients seeking authentication over the listed port. |

| | |
|---|---|
| Guest VLAN | Lists the guest VLAN utilized for the listed port. This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled. |
| Host | Lists whether the host is a single entity or not. |
| Pstatus | Lists whether the listed port has been authorized for Dot1x network authentication. |

Refer to the **MacAuth** table to assess the AAA policy applied to MAC authorization requests.

Review the following **MAC Auth Ports** utilization information:

| | |
|---|---|
| Name | Lists the controller or service platform GE ports subject to automatic connection and MAC authentication using Dot1x. |
| Authorized | Lists whether MAC authorization using Dot1x has been authorized (permitted) on the listed GE port. A green checkmark designates Dot1x authorization as authorized. A red X defines authorization as disabled. |
| Enabled | Lists whether MAC authorization using Dot1x has been or enabled)on the listed GE port. A green checkmark designates Dot1x authorization as allowed. A red X defines authorization as disabled. |
| MAC Auth | Lists the port's factory encoded MAC address. |

5 Select **Refresh** to update the screen's statistics counters to their latest value.

## AP Network

Use the **Network** screens to view information impacting access point ARP (hardware address determination), routing, bridging, IGMP, DHCP Cisco and link layer discovery utilization statistics.

For more information, refer to the following:


- AP Network ARP Entries on page 1039
- AP Network Route Entries on page 1040
- AP Network Default Routes on page 1042
- AP Network Bridge on page 1044
- AP Network IGMP on page 1046
- AP Network MLD on page 1047
- AP Network Traffic Shaping on page 1049
- AP Network DHCP Options on page 1050
- AP Network Cisco Discovery Protocol on page 1051
- AP Network Link Layer Discovery Protocol on page 1052
- AP Network IPv6 Neighbor on page 1054
- AP Network MSTP on page 1055

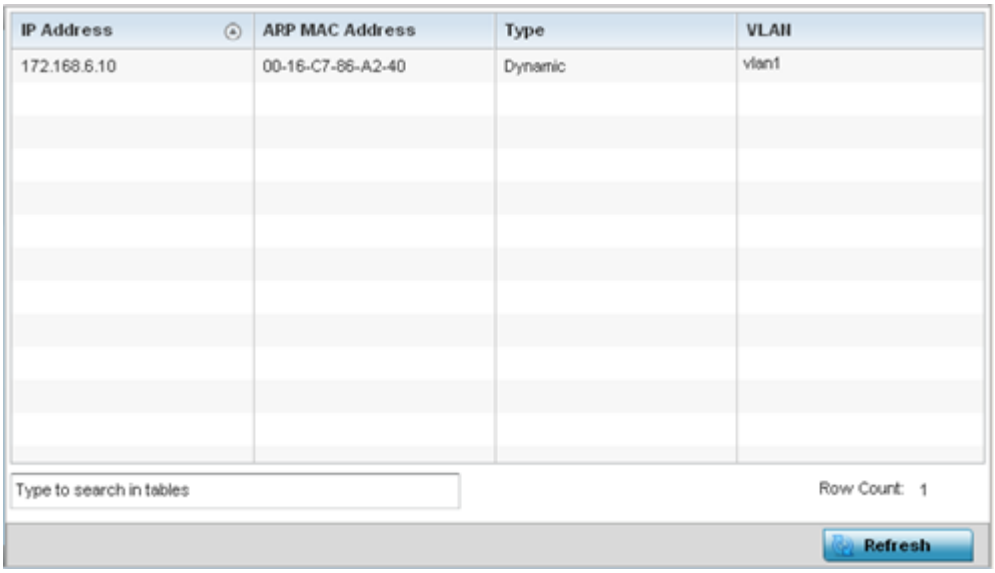

### *AP Network ARP Entries*

ARP *(Address Resolution Protocol)* is a protocol for mapping an IP address to a device address recognized in the local network. An address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

To view the ARP entries on the network statistics screen:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI..
5 Select **ARP Entries**.

The **Statistics > AP > Network > ARP Entries**s screen is displayed.




The ARP Entries screen displays the following:

| | |
|---|---|
| IP Address | Displays the IP address of the client being resolved on behalf of the controller or service platform. |
| ARP MAC Address | Displays the MAC address of the device where an IP address is being resolved. |
| Type | Defines whether the entry was added statically or created dynamically in respect to network traffic. Entries are typically static. |
| VLAN | Displays the name of the VLAN ID where the IP address was found. |

6 Select the **Refresh** button to update the screen's statistics counters to their latest values.

*AP Network Route Entries*

The Route Entries screen displays the destination subnet, gateway, and interface for routing packets to a defined destination. When an existing destination subnet does not meet the needs of the network, add a new destination subnet, subnet mask and gateway.

To view route entries:

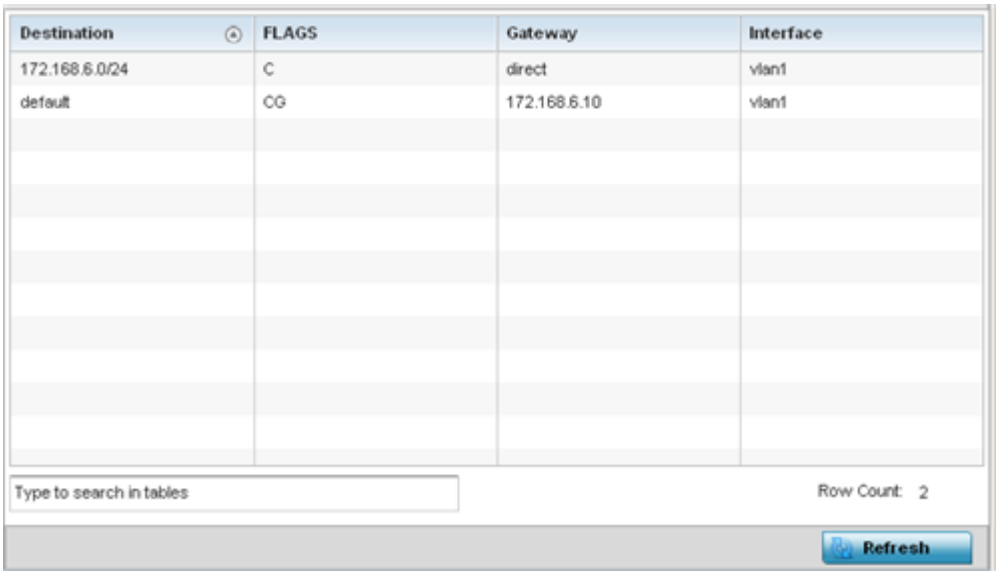
1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Network** menu from the left-hand side of the UI.

5 Select **Route Entries**.

The **Statistics > AP > Network > IPv4 Route Entries** screen is displayed.

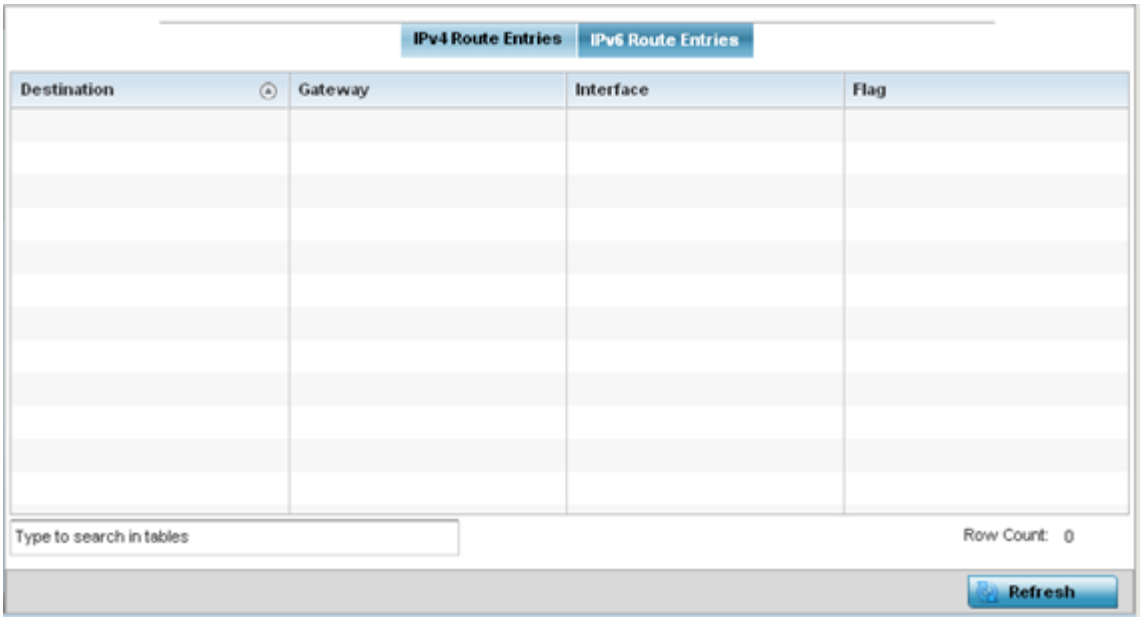



The IPv4 Route Entries screen provides the following information:

| | |
|---|---|
| Destination | Displays the IPv4 formatted address of the destination route address. |
| Distance | Lists the hop distance to a desired route. Devices regularly send neighbors their own assessment of the total cost to get to all known destinations. A neighboring device examines the information and compares it to their own routing data. Any improvement on what's already known is inserted in that device's own routing tables. Over time, each networked device discovers the optimal next hop for each destination. |
| Route | Lists the IPv4 formatted IP address used for routing packets to a defined destination. |
| Flags | The flag signifies the condition of the direct or indirect route. |
| Gateway | Displays the gateway IP address used to route packets to the destination subnet. |
| Interface | Displays the name of the controller interface or VLAN utilized by the destination subnet. |
| Metric | Lists the metric (or cost) of the route to select (or predict) the best route. The metric is computed using a routing algorithm, and covers information bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost. |

6 Select the **IPv6 Route Entries** tab to review route data for IPv6 formatted traffic.

The IPv6 Route Entries stats display in the right-hand pane.




The IPv6 Route Entries screen provides the following information:

| | |
|---|---|
| Destination | Displays the IPv6 formatted address of the destination route address. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| Gateway | Displays the gateway IP address used to route packets to the destination subnet. |
| Interface | Displays the name of the controller interface or VLAN utilized by the destination subnet. |
| Flag | The flag signifies the condition of the direct or indirect route. |

7 Select **Refresh** to update the display to the latest values.

*AP Network Default Routes*

In an IPv6 supported environment unicast routing is always enabled. A controller or service platform routes IPv6 formatted traffic between interfaces as long as the interfaces are enabled for IPv6 and ACLs allow IPv6 formatted traffic. However, an administrator can add a default routes as needed.

Static routes are manually configured. They work fine in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.

To view access point's default routes:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

The System node expands to display the RF Domains created within the managed network.

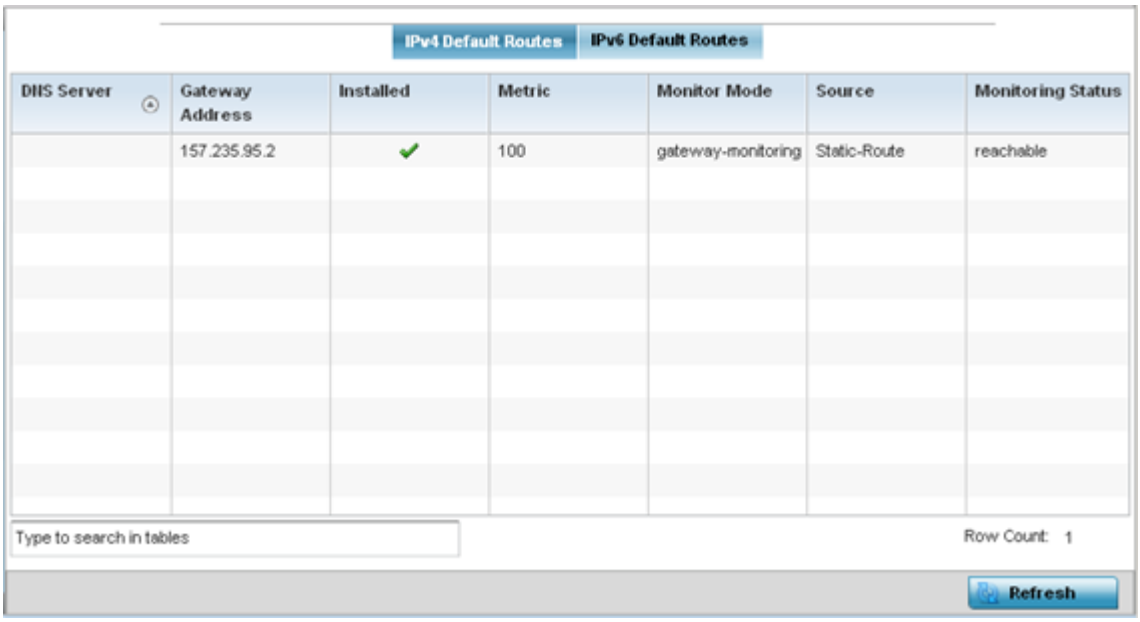
3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Network** menu from the left-hand side of the UI.

5 Select **Route Entries**.

The **Statistics > AP > Network > IPv4 Default Routes** screen is displayed.

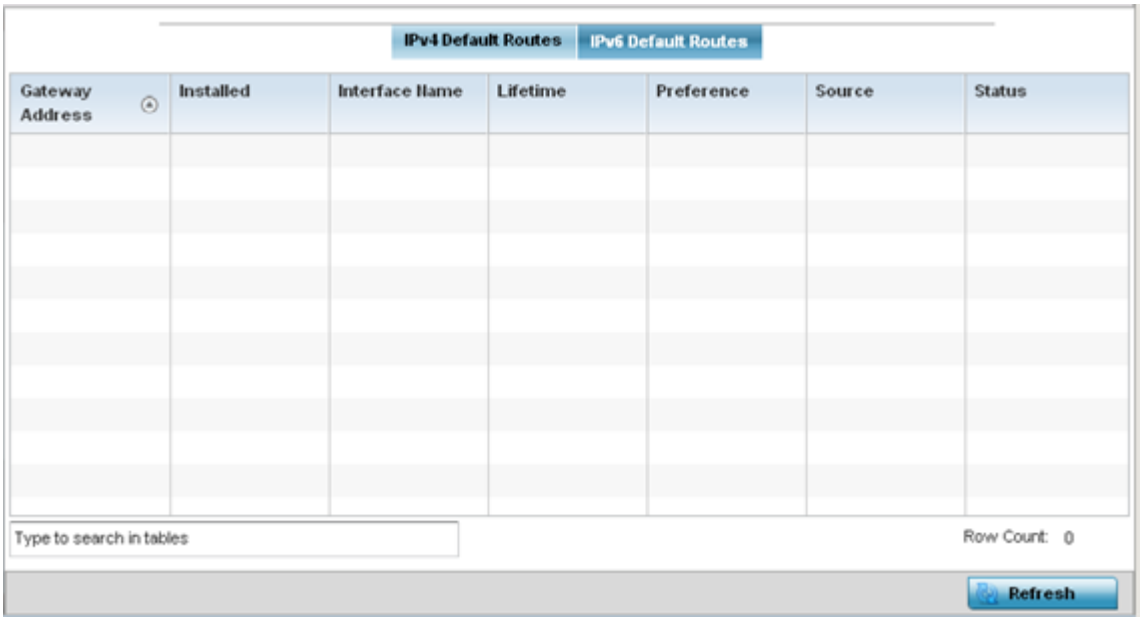



The IPv4 Default Routes screen provides the following information:

| | |
|---|---|
| DNS Server | Lists the address of the DNS server providing IPv4 formatted address assignments on behalf of the access point. |
| Gateway | Lists the IP address of the gateway resource used with the listed route. |
| Installed | A green checkmark defines the listed route as currently installed on the access point. A red X defines the route as not currently installed and utilized. |
| Metric | The metric (or cost) could be the distance of a router (round-trip time), link throughput or link availability. |
| Monitor Mode | Displays where in the network the route is monitored for utilization status. |
| Source | Lists whether the route is static or an administrator defined default route. Static routes are manually configured. Static routes work adequately in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table. |
| Monitoring Status | Lists whether the defined IPv4 route is currently reachable on the access point managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized. |

6 Select the **IPv6 Default Routes** tab to review default route availabilities for IPv6 formatted traffic.

The **Statistics > AP > Network > IPv6 Default Routes** stats is displayed by default in the right-hand pane.




| | |
|---|---|
| Gateway Address | Lists the IP address of the gateway resource used with the listed route. |
| Installed | A green checkmark defines the listed IPv6 default route as currently installed on the access point. A red X defines the route as not currently installed and utilized. |
| Interface Name | Displays the interface on which the IPv6 default route is being utilized. |
| Lifetime | Lists the lifetime representing the valid usability of the default IPv6 route. |
| Preference | Displays the administrator defined IPv6 preferred route for IPv6 traffic. |
| Source | Lists whether the route is static or an administrator defined default route. Static routes are manually configured. Static routes work adequately in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table. |
| Status | Lists whether the defined IPv6 route is currently reachable on the access point managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized. |

7 Select **Refresh** to update the display to the latest values.

## *AP Network Bridge*

*Bridging* is a forwarding technique making no assumption about where a particular network address is located. It depends on flooding and the examination of source addresses in received packet headers to locate unknown devices. Once a device is located, its location is stored in a table to avoid broadcasting to that device again. Bridging is limited by its dependency on flooding, and is used in local area networks only. A bridge and a controller are very similar, since a controller is a bridge with a number of ports.

The **Bridge** screen provides details about the IGS *(Integrate Gateway Server )*, which is a router connected to an access point. The IGS performs the following:

- *Issues IP addresses*
- *Throttles bandwidth*

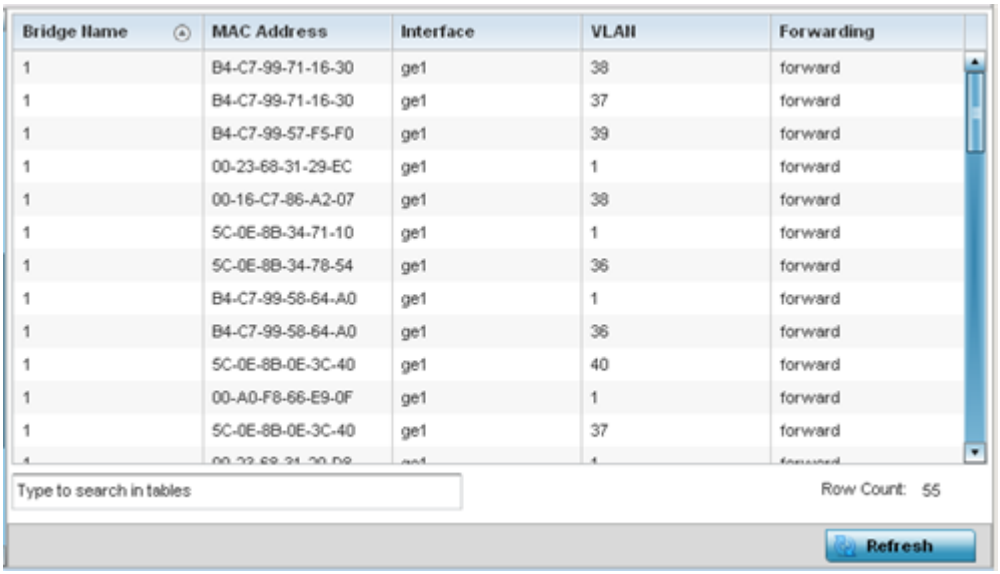
- *Permits access to other networks*
- *Times out old logins*

This screen also provides information about the MRouter *(Multicast Router)*, which is a router program that distinguishes between multicast and unicast packets and how they should be distributed along the Multicast Internet. Using an appropriate algorithm, a multicast router instructs a switching device what to do with the multicast packet.

To view an access point's Bridge statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **Bridge**.

The **Statistics > AP > Bridge** stats is displayed in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| Bridge Name | Displays the numeric ID of the network bridge. |
| MAC Address | Displays the MAC address (factory encoded hardware identifier) of the bridge. |
| Interface | Displays the interface (access point physical port name) where the bridge transferred packets. Supported access points models have different port configurations. |
| VLAN | Displays the VLAN the bridge is using as a virtual interface within the network. |
| Forwarding | Displays whether the bridge is forwarding packets and is in a forwarding state. A bridge can only forward packets. |

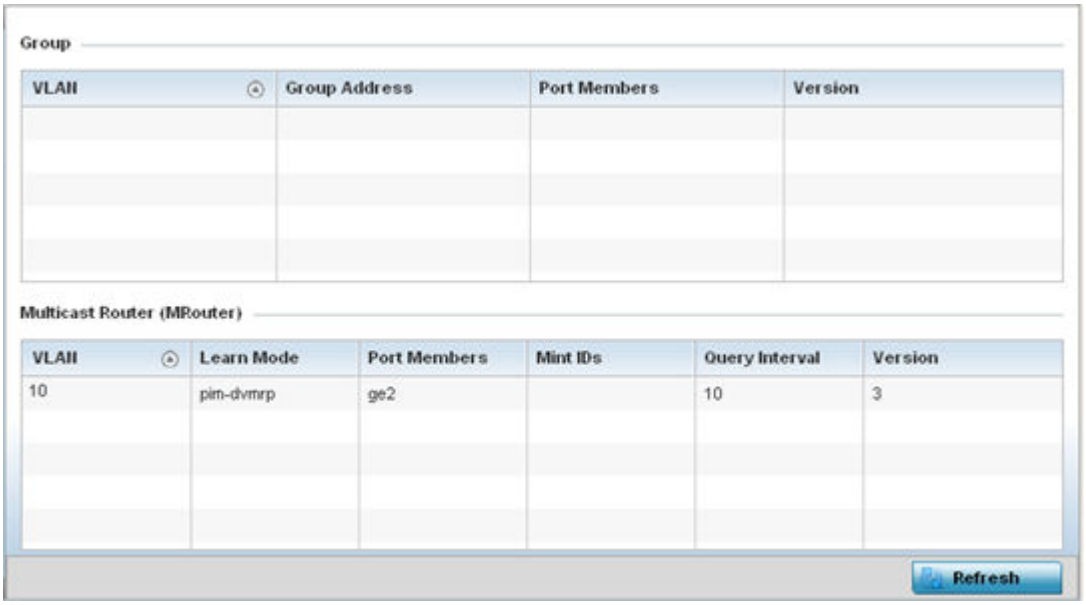
6 Select **Refresh** to update the counters to their latest values.

*AP Network IGMP*

IGMP is a protocol used for managing members of IP multicast groups. An access point listens to IGMP network traffic and forwards IGMP multicast packets to radios on which interested hosts are connected. On the wired side of the network, the access point floods all the wired interfaces. IGMP reduces unnecessary multicast traffic floods within the network and help reduce administrative overhead.

To view a AP-managed network's IGMP configuration:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **IGMP**.




The **Group** field describes the following:

| | |
|---|---|
| VLAN | Displays the group VLAN where the multicast transmission is conducted. |
| Group Address | Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to. |
| Port Members | Displays the ports on which multicast clients have been discovered. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models. |
| Version | Displays each listed group IGMP version compatibility as either version 1, 2 or 3. |

The **Multicast Router (MRouter)** field describes the following:

| | |
|---|---|
| VLAN | Displays the group VLAN where the multicast transmission is conducted. |
| Learn Mode | Displays the learning mode used by the router as either **`Static`** or **`PIM-DVMRP`**. |

| | |
|---|---|
| Port Members | Displays the physical ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models. |
| MiNT IDs | Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure access point profile communications at the transport layer. Using MiNT, an access point can be configured to only communicate with other authorized (MiNT enabled) access points of the same model. |
| Query Interval | Lists the IGMP query interval implemented when the querier functionality is enabled. The default value is 60 seconds. |
| Version | Lists the multicast router IGMP version compatibility as either version 1, 2 or 3. The default setting is 3. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

### *AP Network MLD*

MLD snooping enables a controller, service platform or Access Point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or Access Point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or Access Point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

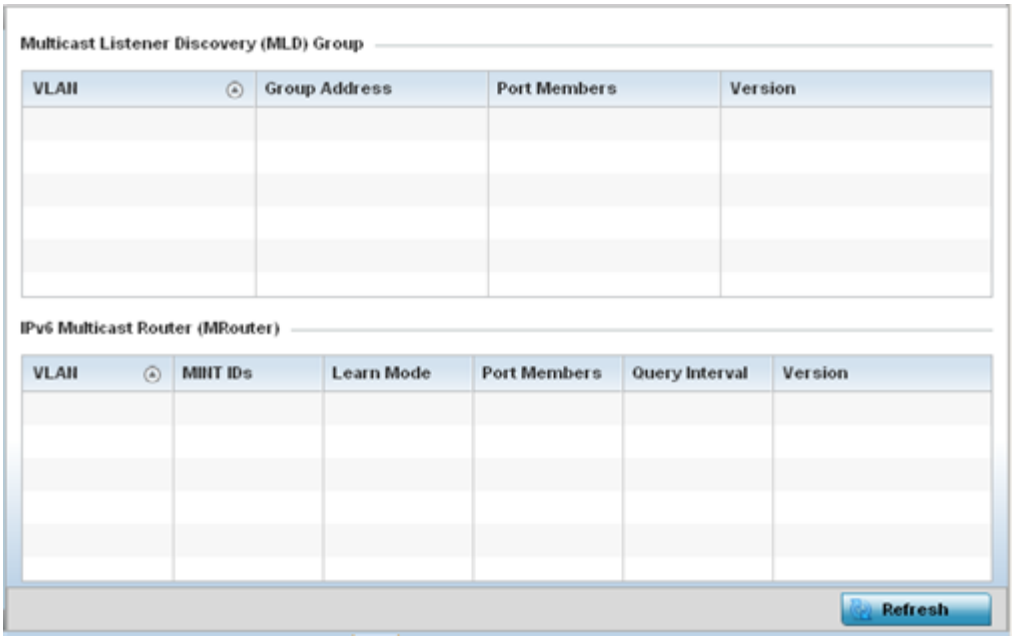
To view network MLD statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

  The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points.

  The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **MLD**.

  The **Statistics > AP > MLD** stats is displayed in the right-hand pane.




The **Multicast Listener Discovery (MLD) Group** field describes the following:

| | |
|---|---|
| VLAN | Displays the group VLAN where the MLD groups multicast transmission is conducted. |
| Group Address | Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to. |
| Port Members | Displays the ports on which MLD multicast clients have been discovered. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models. |
| Version | Displays each listed group's version compatibility as either version 1, 2 or 3. |

The **IPv6 Multicast Router (MRouter)** field describes the following:

| | |
|---|---|
| VLAN | Displays the group VLAN where the multicast transmission is conducted. |
| MINT IDs | Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure communications at the transport layer. Using MiNT, a controller or service platform can be configured to only communicate with other authorized (MiNT enabled) devices. |
| Learn Mode | Displays the learning mode used by the router as either **`Static`** or **`PIM-DVMRP`**. |
| Port Members | Displays the physical ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models. |
| Query Interval | Lists the query interval implemented when the querier functionality is enabled. The default value is 60 seconds. |
| Version | Lists the multicast router version compatibility as either version 1, 2 or 3. The default setting is 3. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP Network Traffic Shaping*

Traffic shaping regulates network data transfers to ensure a specific performance level. Traffic shaping delays the flow of packets defined as less important than prioritized traffic streams. Traffic shaping enables traffic control out an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms applied policies. Traffic can be shaped to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, an application takes precedence over an application category, then ACLs.


- Traffic Shaping - Status on page 1049
- Traffic Shaping - Statistics on page 1049


**Traffic Shaping - Status**

To view network Access Point traffic shaping status:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **Traffic Shaping**.

The **Statistics > AP > Traffic Shaping > Status** screen displays by default.

The status screen simply lists the AP's current traffic shaping operational status.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

**Traffic Shaping - Statistics**

To view network Access Point traffic shaping statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

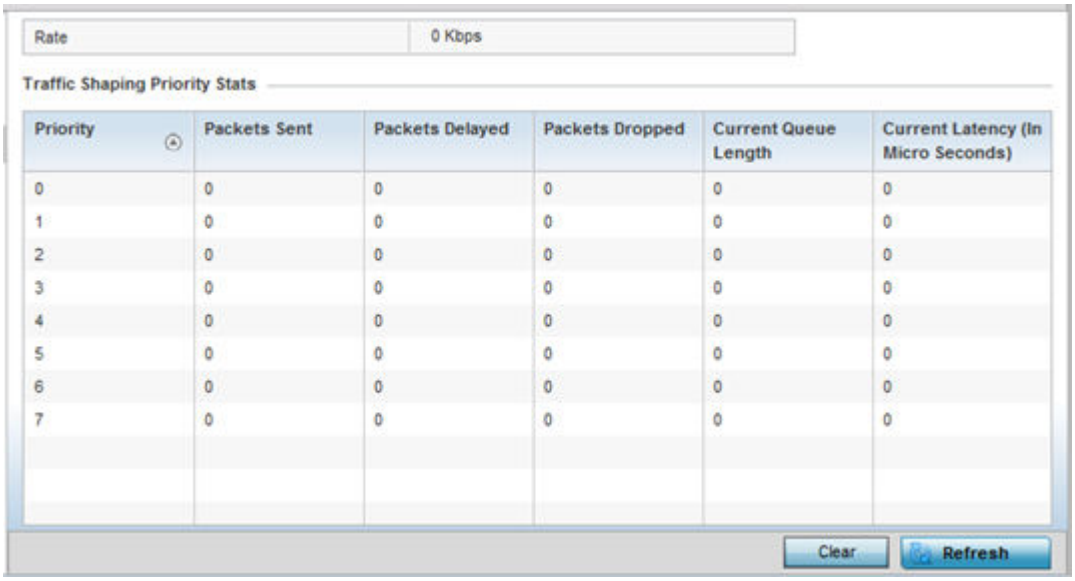
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **Traffic Shaping**.

The **Statistics > AP > Traffic Shaping > Statistics** screen is displayed.




This screen displays the following information:

| | |
|---|---|
| Rate | The rate configuration controls the maximum traffic rate sent or received on an interface. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority. |
| Priority | Lists the traffic shaper queue priority. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets 802.1p markings. |
| Packets Sent | Provides a baseline of the total number of packets sent to assess packet delays and drops as a result of the filter rules applied in the traffic shaping configuration. |
| Packets Delayed | Lists the packets defined as less important than prioritized traffic streams and delayed as a result of traffic shaping filter rules applied. |
| Packets Dropped | Lists the packets defined as less important than prioritized traffic streams, delayed and eventually dropped as a result of traffic shaping filter rules applied. |
| Current Length | Lists the packet length of the data traffic shaped to meet downstream requirements. |
| Current Latency | Traffic shaping latency is the time limit after which packets start dropping as a result of the traffic prioritization filter rules applied. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP Network DHCP Options*

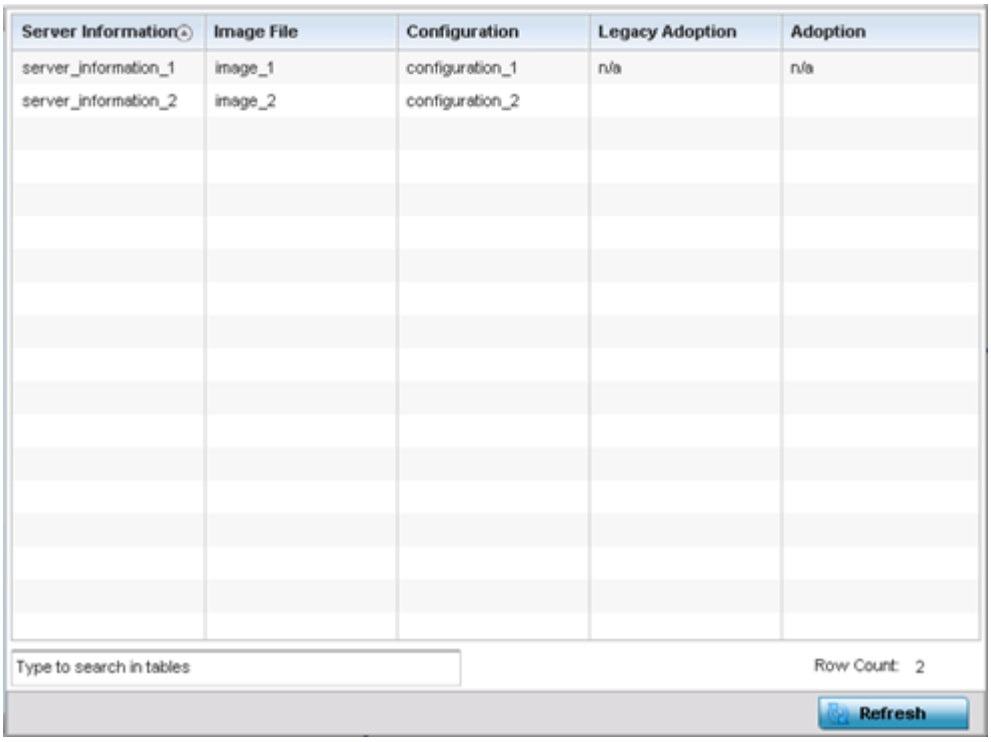
Supported access points can use internal or external DHCP server resources to provide the dynamic assignment of IP addresses to requesting clients. DHCP is a protocol that includes IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, gateway and network mask.

The DHCP Options screen provides the DHCP server name, image file on the DHCP server, and its configuration.

To view a network's DHCP Options:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **DHCP Options**.

The **Statistics > AP > Network > DHCP Options** screen displays.




This screen describes the following:

| | |
|---|---|
| Server Information | Displays the DHCP server hostname used on behalf of the access point. |
| Image File | Displays the image file name. BOOTP or the bootstrap protocol can be used to boot diskless clients. An image file is sent from the boot server. The file contains the operating system image. DHCP servers can be configured to support BOOTP. |
| Configuration | Displays the name of the configuration file on the DHCP server. |
| Legacy Adoption | Displays legacy (historical) device adoption information on behalf of the access point. |
| Adoption | Displays pending (current) adoption information on behalf of an access point. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

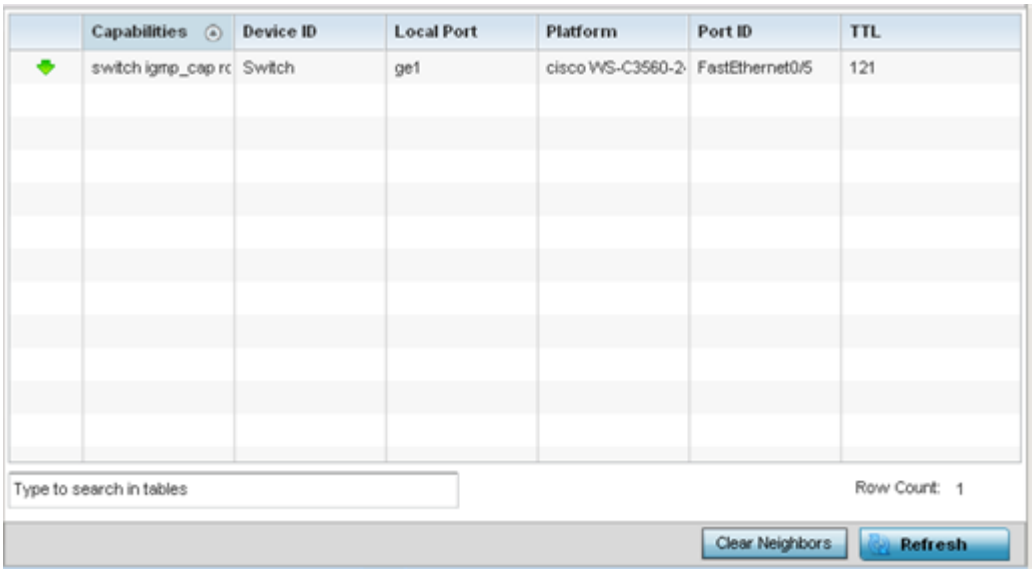
### *AP Network Cisco Discovery Protocol*

CDP is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment, and used to share information about network devices.

To view an access point's CDP statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **Cisco Discovery Protocol**.

The **Statistics > AP > Network > Cisco Discovery Protocol** screen displays in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| Capabilities | Displays the capabilities code for CISCO neighbors as either **Router**, **Trans Bridge**, **Source Route Bridge**, **Switch**, **Host**, **IGMP** or **Repeater**. |
| Device ID | Displays the configured device ID or name for each device in the table. |
| Local Port | Displays the local port name (access point physical port) for each CDP capable device. Supported access point models have unique port configurations. |
| Platform | Displays the model number of the CDP capable device interoperating with the access point. |
| Port ID | Displays the access point's numeric identifier for the local port. |
| TTL | Displays the TTL for each CDP connection. |

6 Click **Clear Neighbors** to remove all known CDP neighbors from the table.
7 Select **Refresh** to update the screen's statistics counters to their latest values.

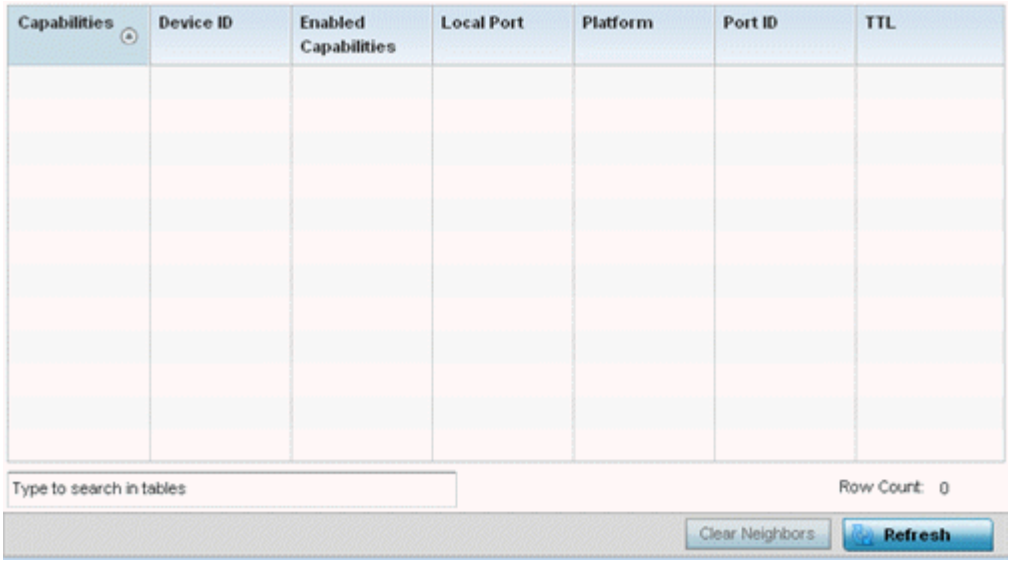
### *AP Network Link Layer Discovery Protocol*

LLDP or IEEE 802.1AB is a vendor-neutral Data Link Layer protocol used by network devices for advertising of (announcing) their identity, capabilities, and interconnections on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery*.

To view a network's Link Layer Discovery Protocol statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **Link Layer Discovery**.

The **Statistics > AP > Network > Link Layer Discovery Protocol** screen displays in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| Capabilities | Displays a capabilities code as either **Router**, **Trans Bridge**, **Source RouteBridge**, **Switch**, **Host**, **IGMP** or **Repeater**. |
| Device ID | Displays the configured device ID or name for each device in the table. |
| Enabled Capabilities | Displays which device capabilities are currently enabled. |
| Local Port | Displays the local port name (access point physical port) for each LLDP capable device. Supported access point models have unique port configurations. |
| Platform | Displays the model number of the LLDP capable device interoperating with the access point. |
| Port ID | Displays the identifier for the local port. |
| TTL | Displays the TTL for each LLDP connection. |

6 Select **Clear Neighbors** to remove all known LLDP neighbors from the table.
7 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP Network IPv6 Neighbor*

IPv6 neighbor discovery uses ICMP messages and solicited multicast addresses to find the link layer address of a neighbor on the same local network, verify the neighbor's reachability and track neighboring devices.

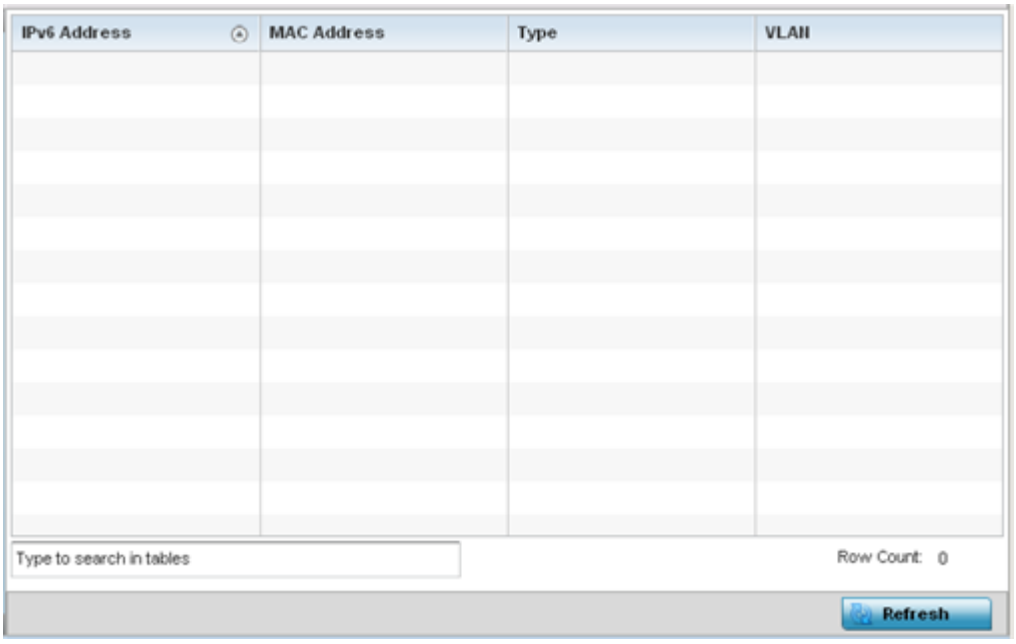
Upon receiving a neighbor solicitation message, the destination replies with NA *(neighbor advertisement)*. The source address in the advertisement is the IPv6 address of the device sending the message. The destination address in the advertisement message is the IPv6 address of the device sending the neighbor solicitation. The data portion of the NA includes the link layer address of the node sending the neighbor advertisement.

Neighbor solicitation messages also verify the availability of a neighbor once its the link layer address is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.

To view an access point's IPv6 neighbor statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).
The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points.
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **IPv6 Neighbor**.
The **Statistics > AP > Network > IPv6 Neighbor Discovery** screen is displayed in the right-hand pane.



This screen displays the following:

| | |
|---|---|
| IPv6 Address | Lists an IPv6 IP address for neighbor discovery. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via CMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. |
| MAC Address | Lists the factory encoded hardware MAC address of the neighbor device using an IPv6 formatted IP address as its network identifier. |
| Type | Displays the device type for the neighbor solicitation. Neighbor solicitations request the link layer address of a target node while providing the sender's own link layer address to the target. Neighbor solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor. Options include **`Host`**, **`Router`** and **`DHCP Server`**. |
| VLAN | Lists the virtual interface (from 1 - 4094) used for the required neighbor advertisements and solicitation messages used for neighbor discovery. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP Network MSTP*

MSTP provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there's just one VLAN in the Access Point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

MSTP includes all of its spanning tree information in a single BPDU format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the Access Point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To view an access point's MSTP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

The System node expands to display the RF Domains created within the managed network.

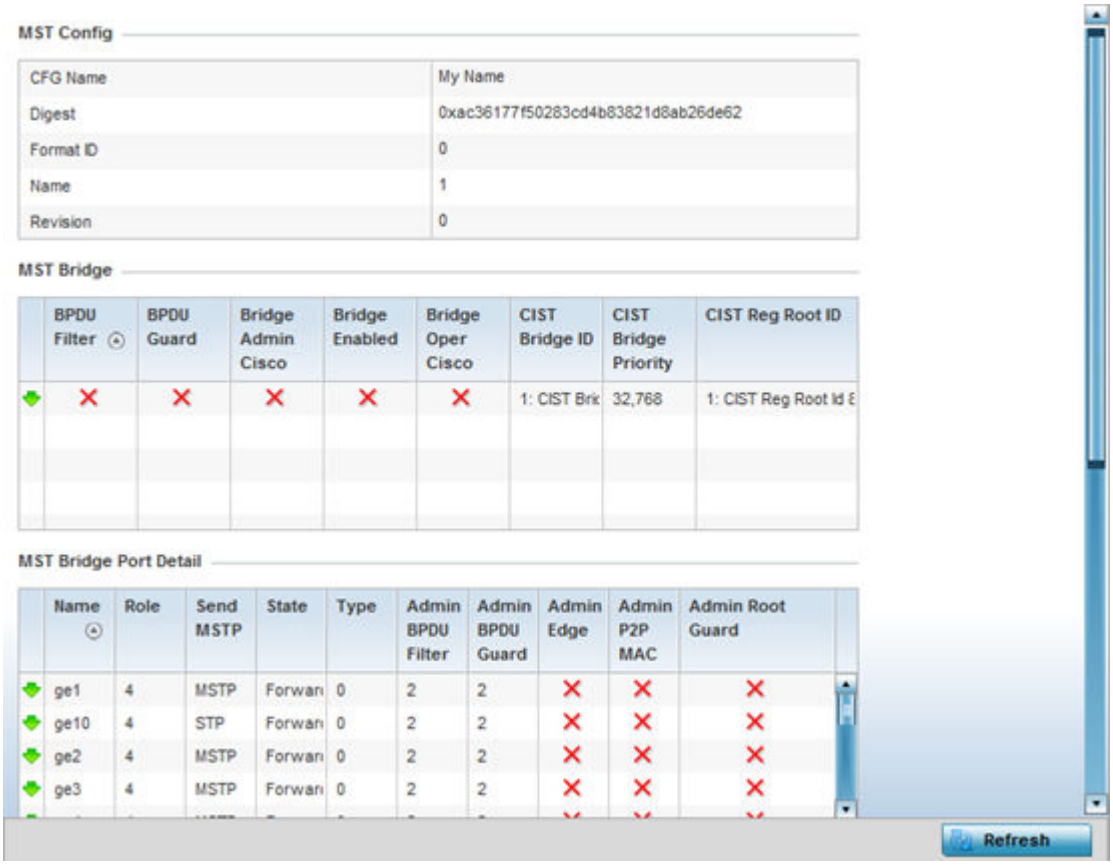
3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Network** menu from the left-hand side of the UI.

5 Select **MSTP**.

The **Statistics > AP > Network > MSTP** screen is displayed in the right-hand pane.




The MST Config field displays the name assigned to the MSTP configuration, its digest, format ID, name and revision.

The MST Bridge field lists the filters and guards that have been enabled and whether Cisco interoperability if enabled.

The MST Bridge Port Detail field lists specific controller or service platform port status and their current state.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP DHCPv6 Relay & Client

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCPv6 relay agents receive messages from clients and forward them a DHCPv6 server. The server sends responses back to the relay agent and the relay agent sends the responses to the client on the local link.

To view the access point's DHCPv6 relay configuration:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

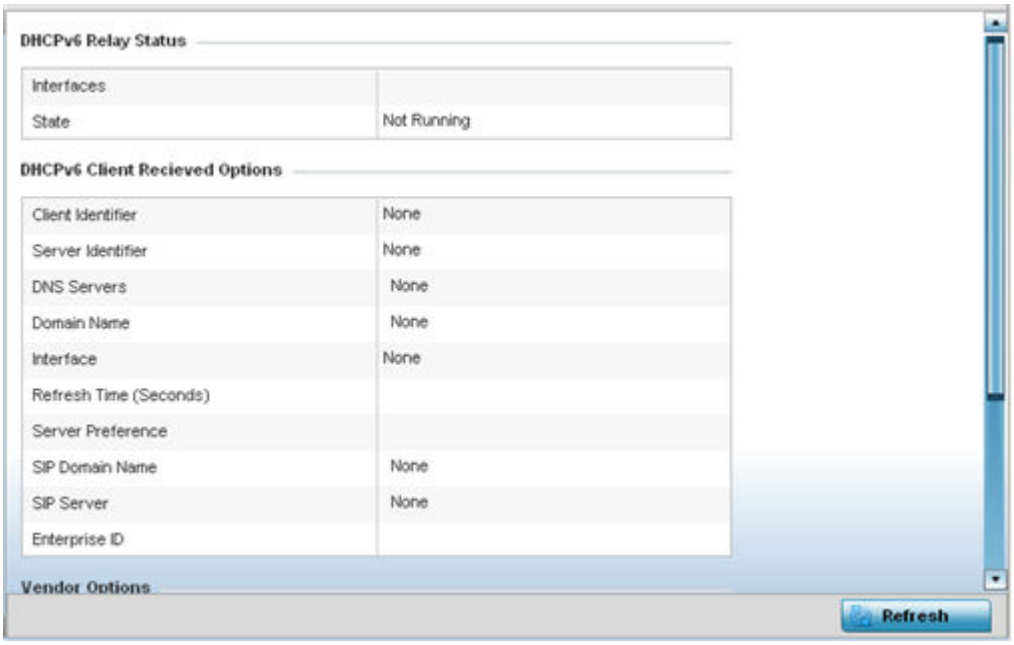
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **DHCPv6 Relay & Client**.

The **Statistics > Controller > DHCP Relay & Client** screen displays in the right-hand pane.




The **DHCP Relay Status** table defines the following:

| | |
|---|---|
| **Interfaces** | Displays the access point interface used for DHCPv6 relay. |
| **State** | Displays the current operational state of the DHCPv6 server to assess its availability as a viable IPv6 provisioning resource. |

The **DHCPv6 Client Received Options** table defines the following:

| | |
|---|---|
| **Client Identifier** | Lists whether the reporting client is using a *hardware address* or *client identifier* as its identifier type within requests to the DHCPv6 server. |
| **Server Identifier** | Displays the server identifier supporting client DHCPv6 relay message reception. |
| **DNS Servers** | Lists the DNS server resources supporting relay messages received from clients. |
| **Domain Name** | Lists the domain to which the remote server resource belongs. |
| **Interface** | Displays the interfaces dedicated to client DHCPv6 relay message reception. |
| **Refresh Time (Seconds)** | Lists the time (in seconds) since the data populating the DHCPv6 client received options table has been refreshed. |
| **Server Preference** | Lists the preferred DHCPv6 server resource supporting relay messages received from clients. |

| | |
|---|---|
| SIP Domain Name | Lists the SIP domain name supporting DHCPv6 client telephone extensions or voice over IP systems. |
| SIP Server | Displays the SIP server name supporting DHCPv6 telephone extensions or voice over IP systems. |
| Enterprise ID | Lists the enterprise ID associated with DHCPv6 received client options. |

Refer to the Vendor Options table for the following:

| | |
|---|---|
| Code | Lists the relevant numeric DHCP vendor code. |
| Data | Lists the supporting data relevant to the listed DHCP vendor code. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP DHCP Server

Access points' utilize an internal DHCP server. DHCP can provide IP addresses automatically to requesting wireless clients. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters (IP address, network mask gateway, etc.) from a DHCP server to a client.

To review DHCP server statistics, refer to the following:

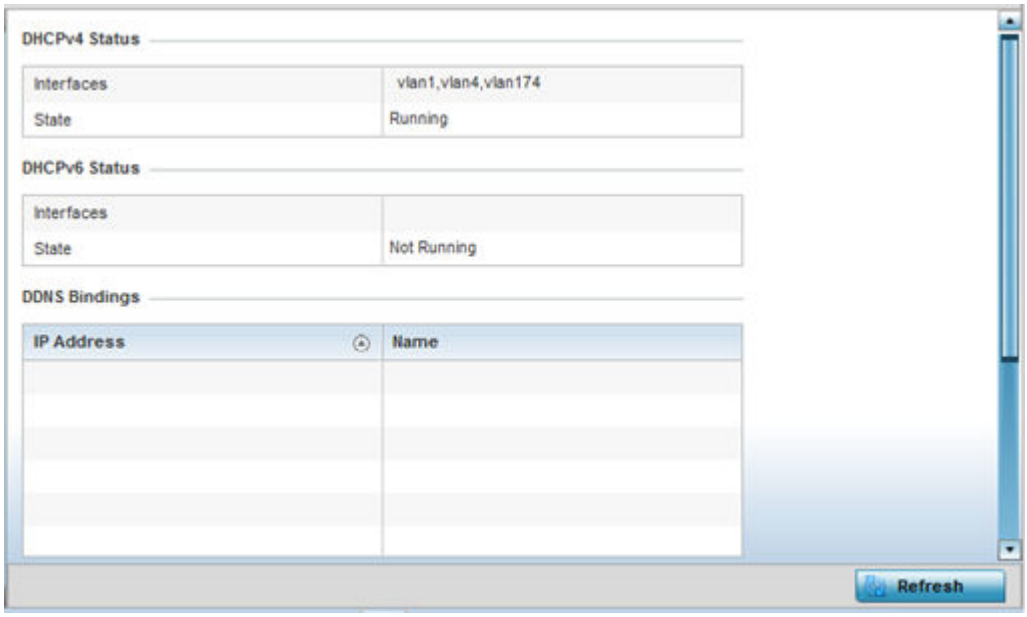
- AP DHCP - General on page 1058
- AP DHCP - Bindings on page 1059
- AP DHCP - Networks on page 1060

### *AP DHCP - General*

To view General DHCP status and binding information:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **DHCP Server** menu.

The **Statistics > AP > DHCP Server > General** screen displays by default in the right-hand pane.




The DHCPv4 Status and DHCPv6 Status tables defines the following:

| | |
|---|---|
| Interfaces | Displays the access point interface used with the DHCPv4 or DHCPv6 resource for IP address provisioning. |
| State | Displays the current operational state of the DHCPv4 or DHCPv6 server to assess its availability as a viable IP provisioning resource. |

The DDNS Bindings table displays the following:

| | |
|---|---|
| IP Address | Displays the IP address assigned to the requesting client. |
| Name | Displays the domain name mapping corresponding to the listed IP address. |

The DHCP Manual Bindings table displays the following:

| | |
|---|---|
| IP Address | Displays the IP address for clients requesting DHCP provisioning resources. |
| Client Id | Displays the client's ID used to differentiate requesting clients. |

*AP DHCP - Bindings*

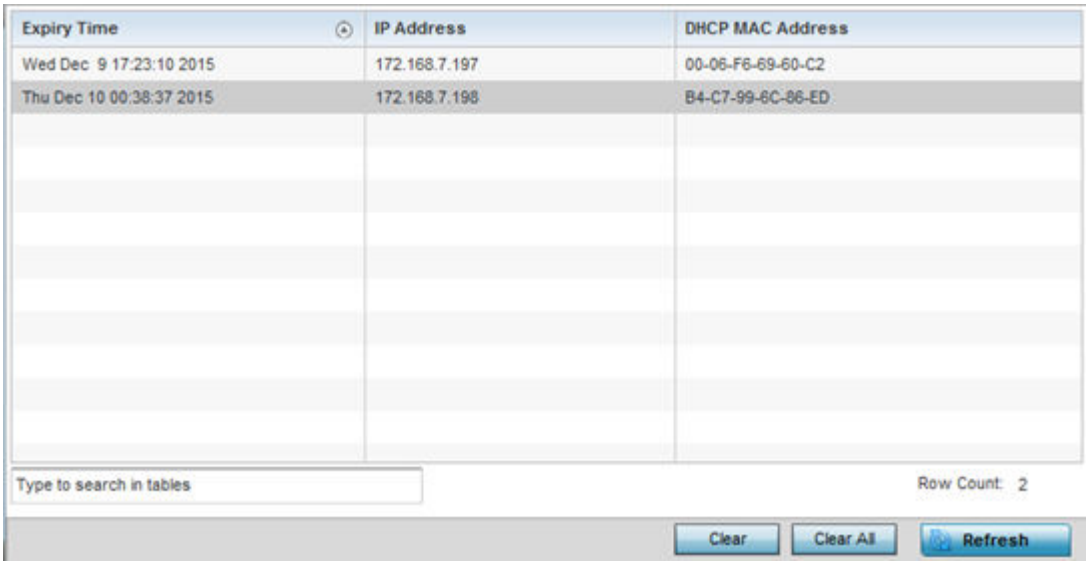
The DHCP Binding displays DHCP binding information such as expiry time, client IP addresses and their MAC address.

Access points build and maintain a DHCP snooping table (DHCP binding database). An access point uses the snooping table to identify and filter untrusted messages. The DHCP binding database keeps track of DHCP addresses assigned to ports, as well as filtering DHCP messages from untrusted ports. Incoming packets received on untrusted ports, are dropped if the source MAC address does not match the MAC in the binding table.

To view a network's DHCP Bindings:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **DHCP Server** menu.
5 Select **Bindings**.

The **Statistics > AP > DHCP Server > Bindings** screen displays by default in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| Expiry Time | Displays the expiration of the lease used by the devices requesting controller or service platform DHCP resources. |
| IP Address | Displays the IP address of each listed device requesting DHCP services. |
| DHCP MAC Address | Displays the MAC address of each device requesting DHCP services. |

6 Select a table entry and select **Clear** to remove the client from the list of devices requesting DHCP services.
7 Select **Clear All** to remove all listed clients from the list of requesting clients.
8 Select the **Refresh** button to update the screen's statistics counters to their latest values.

*AP DHCP - Networks*

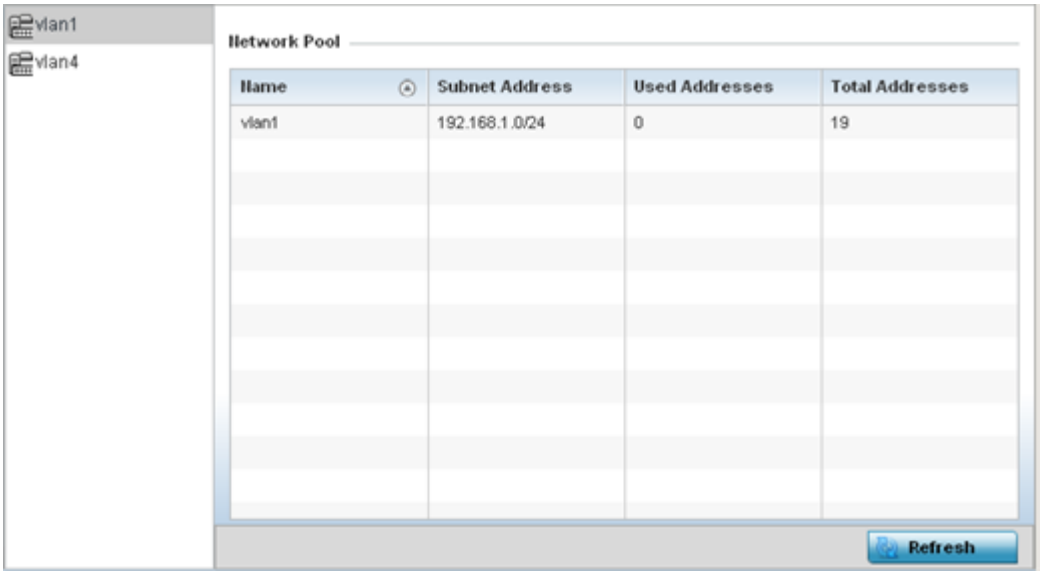
A controller, service platform or access point's DHCP server maintains a pool of IP addresses and client configuration parameters (default gateway, domain name, name servers, etc). On receiving a valid client request, the DHCP server assigns an IP address, a lease (the validity of time), and other IP configuration parameters to a client on an administrator assigned lease basis.

The Networks screen provides network pool information, such as the subnet for the addresses you want to lease from the pool, the pool name, used addresses and the total number of addresses available for lease to a requesting client.

To view the DHCP Server's Networks information:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **DHCP Server** menu.
5 Select **Networks**.

The **Statistics > AP > DHCP Server > Networks** screen displays in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| Name | Displays the name of the virtual network from which IP addresses can be issued to DHCP client requests on the listed controller or service platform interface. |
| Subnet Address | Displays the subnet for the IP addresses used from the network pool. |
| Used Addresses | Displays the number of host IP addresses allocated by the DHCP server. |
| Total Addresses | Displays the total number of IP addresses available in the network pool for requesting clients. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Firewall

A *firewall* is a wireless network security mechanism designed to block unauthorized access while permitting authorized device communications. Firewalls use a set of *permit* or *deny* filters to manage access point resource requests based on a set of administrator defined rules.

The access point's firewall statistics are partitioned into the following:

- Packet Flows
- Denial of Service
- IP Firewall Rules
- MAC Firewall Rules

- NAT Translations
- DHCP Snooping

### *AP Firewall Packet Flows*

The **Packet Flows** screen displays data traffic packet flow utilization. The chart represents the different protocol flows supported, and displays a proportional view of the flows in respect to their percentage of data traffic utilized.

The **Total Active Flows** graph displays the total number of flows supported. Other bar graphs display for each individual packet type.

To view access point packet flows statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **Firewall** menu.

The **Statistics > AP > Firewall > Packet Flows** screen displays by default in the right-Hand pane.


5 Select **Clear All** to revert the statistics counters to zero and begin a new data collection, or select **Refresh** to update the display to the latest values.

### *AP Denial of Service*

A DoS attack or distributed denial-of-service attack is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out a DoS attack may vary, it generally consists of concerted efforts to prevent an Internet site or service from functioning efficiently.

One common method involves saturating the target's machine with external communications requests, so it cannot respond to legitimate traffic or responds so slowly as to be rendered effectively unavailable.

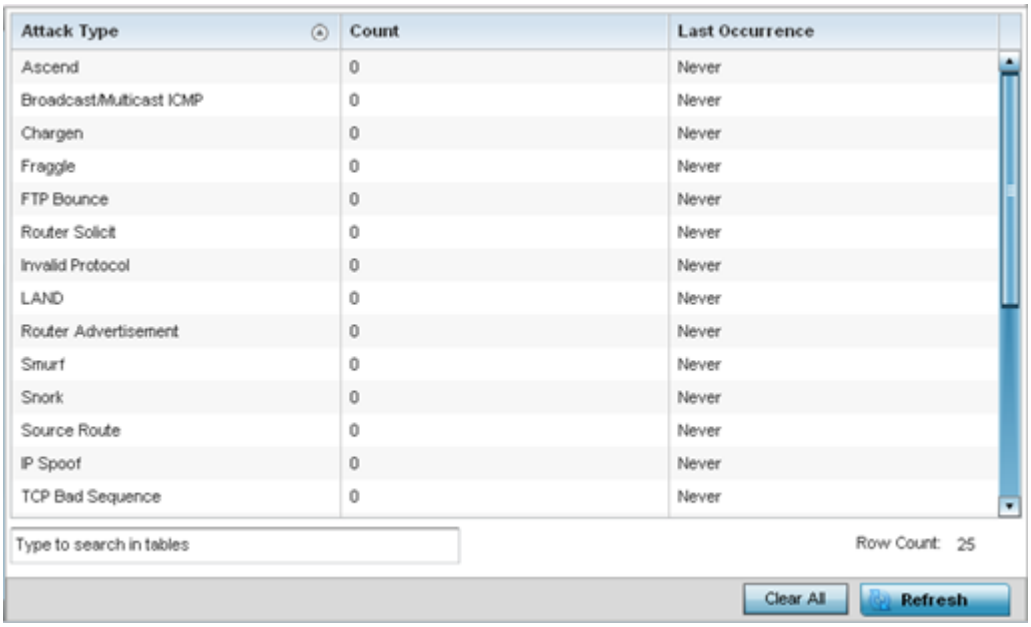
DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consume its resources so it can't provide its intended service.

The DoS screen displays the types of attack, number of times it occurred and the time of last occurrence.

To view an access point's DoS attack configuration:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Firewall** menu.
5 Select **Denial of Service**.

The **Statistics > AP > Firewall > Denial of Service** screen displays in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| Attack Type | Displays the DoS attack type. |
| Count | Displays the number of times the access point's firewall has detected each listed DoS attack. |
| Last Occurrence | Displays when the attack event was last detected by the access point firewall. |

6 Select **Clear All** to revert the statistics counters to zero and begin a new data collection.
7 Select the **Refresh** button to update the screen's statistics counters to their latest values.

*AP IPv4 Firewall Rules*

Create firewall IP address rules to let any computer send or receive traffic from, programs, system services, computers or users. IP firewall rules can be created to provide one of the three actions listed below:

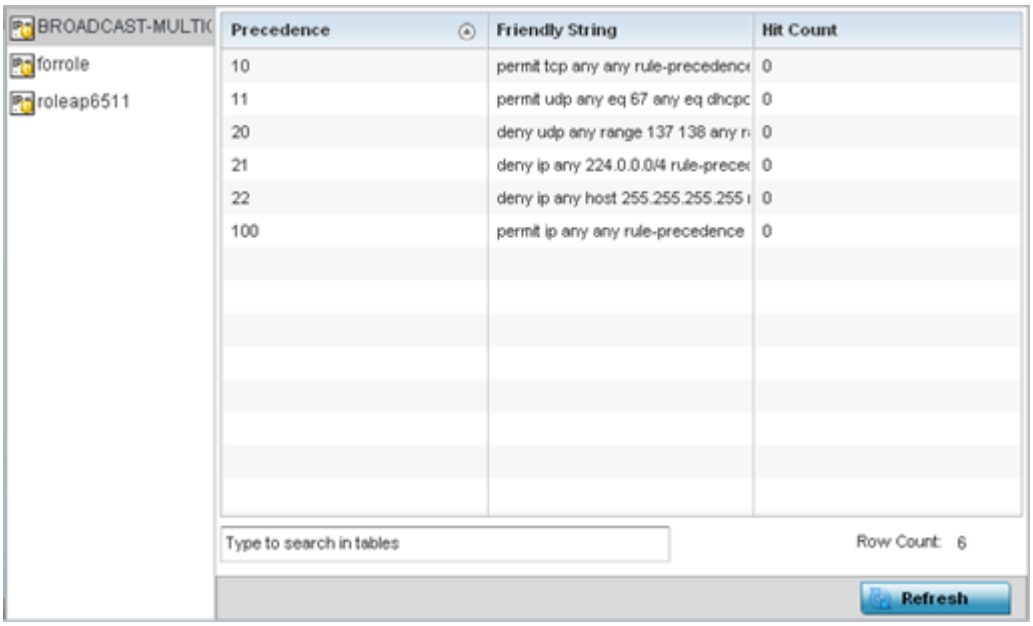
- *Allow a connection*.
- *Allow a connection only if it is secured through the use of Internet Protocol security*.
- *Block a connection*.

Rules can be created for either *inbound* or *outbound* traffic.

To view an access point's IP firewall rules:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Firewall** menu.
5 Select **IP Firewall Rules**.

The **Statistics > AP > Firewall > IP Firewall Rule** screen displays in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| **Precedence** | Displays the precedence (priority) applied to packets. Every rule has a unique precedence value between 1 - 5000. You cannot add two rules with the same precedence value. |
| **Friendly String** | This is a string that provides more information as to the contents of the rule. |
| **Hit Count** | Displays the number of times each WLAN ACL has been triggered. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP IPv6 Firewall Rules*

IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the ND protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

Firewall rules can use one of the three following actions based on a rule criteria:

- *Allow an IPv6 formatted connection*.
- *Allow a connection only if it is secured through the use of IPv6 security*.
- *Block a connection and exchange of IPv6 formatted packets*.

To view an access point's existing IPv6 firewall rules:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

The System node expands to display the RF Domains created within the managed network.

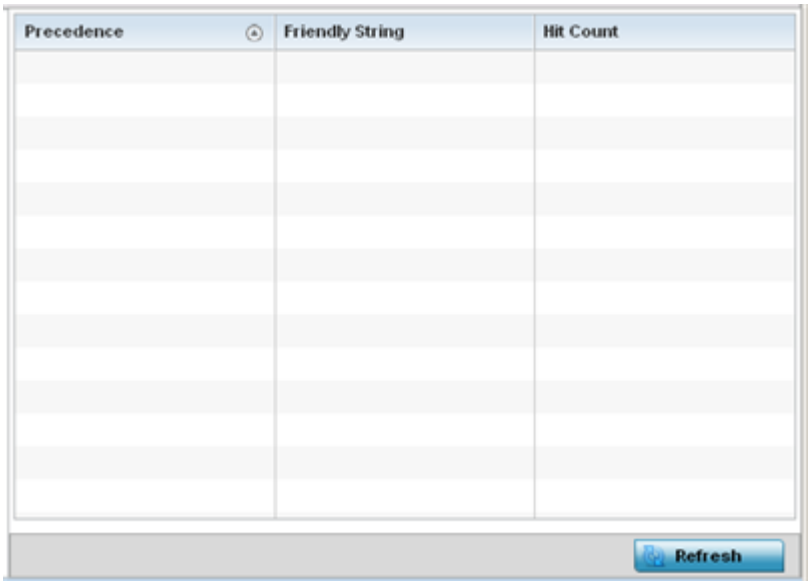
3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Firewall** menu.

5 Select **IPv6 Firewall Rules**.

The **Statistics > AP > Firewall > IPv6 Firewall Rules** screen displays in the right-hand pane.




This screen displays the following information:

| | |
|---|---|
| Precedence | Displays the precedence (priority) applied to IPV6 formatted packets. Unlike IPv4, IPV6 provides enhanced identification and |

| | |
|---|---|
| | location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Every rule has a unique precedence value between 1 - 5000. You cannot add two rules with the same precedence value. |
| Friendly String | This is a string that provides more information as to the contents of the IPv6 specific IP rule. This is for information purposes only. |
| Hit Count | Displays the number of times each IPv6 ACL has been triggered. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP MAC Firewall Rules*

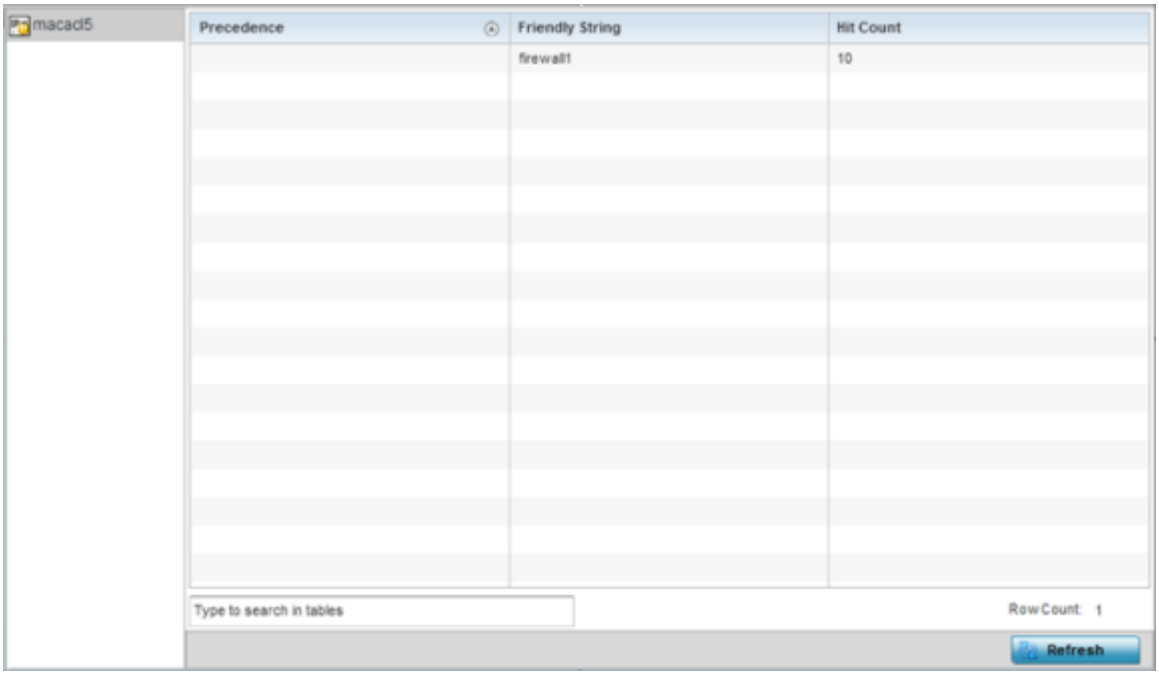
The ability to allow or deny access point connectivity by client MAC address ensures malicious or unwanted clients are unable to bypass the access point's security filters. Firewall rules can be created to support one of the three actions listed below that match the rule's criteria:

- *Allow a connection*.
- *Allow a connection only if it's secured through the MAC firewall security*.
- *Block a connection*.

To view the access point's MAC Firewall Rules:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Firewall** menu.
5 Select **MAC Firewall Rules**.

The **Statistics > AP > Firewall > MAC Firewall Rules** screen displays in the right-hand pane.




This screen displays the following:

| | |
|---|---|
| Precedence | Displays the precedence value, which are applied to packets. The rules within an ACL list are based on their precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence value. |
| Friendly String | This string provides more information as to the contents of the rule. This is for information purposes only. |
| Hit Count | Displays the number of times each WLAN ACL has been triggered. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP NAT Translations*

NAT is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller managed network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

NAT can provide a profile outbound Internet access to wired and wireless hosts connected to either an access point or a wireless controller. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows an access point or wireless controller to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

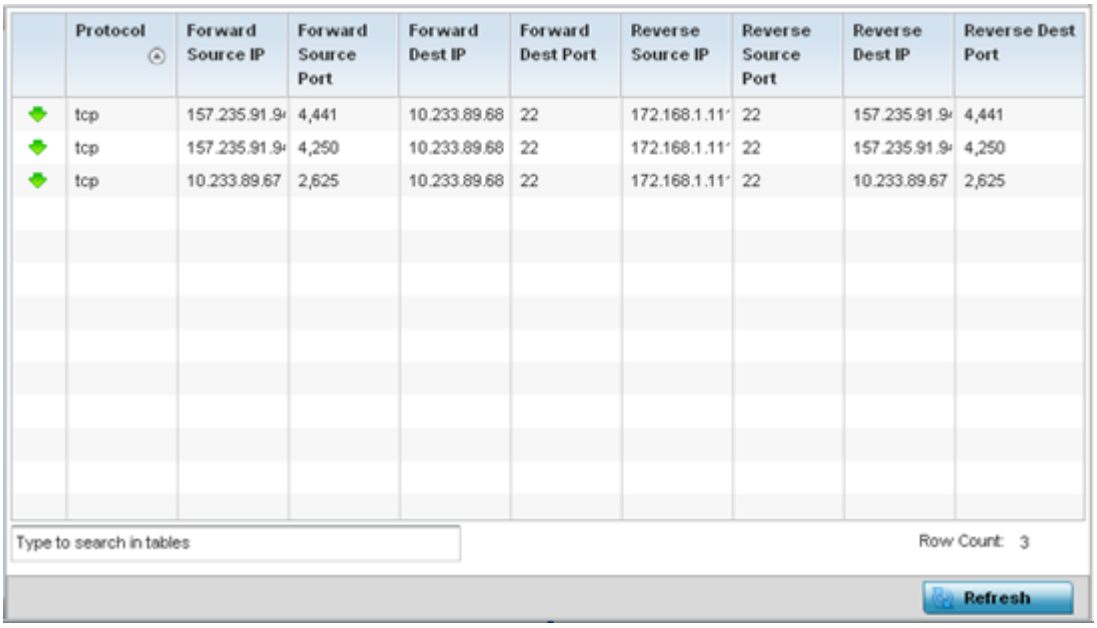
To view the Firewall's NAT translations:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **Firewall** menu.

5 Select **NAT Translations**.

The **Statistics > AP > Firewall > NAT Translations** screen displays in the right-hand pane.




This screen displays the following information:

| | |
|---|---|
| Protocol | Displays the IP translation protocol as either **TCP**, **UDP** or **ICMP**. |
| Forward Source IP | Displays the internal network IP address for forward facing NAT translations. |
| Forward Source Port | Displays the internal network port for forward facing NAT translations. |
| Forward Dest IP | Displays the external network destination IP address for forward facing NAT translations. |
| Forward Dest Port | Displays the external network destination port for forward facing NAT translations. |
| Reverse Source IP | Displays the internal network IP address for reverse facing NAT translations. |
| Reverse Source Port | Displays the internal network port for reverse facing NAT translations. |
| Reverse Dest IP | Displays the external network destination IP address for reverse facing NAT translations. |
| Reverse Dest Port | Displays the external network destination port for reverse facing NAT translations. |

6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP DHCP Snooping*

When DHCP servers are allocating IP addresses to requesting clients on the LAN, DHCP snooping can be configured to better enforce LAN security by allowing only clients with specific IP/MAC addresses.

1 Select the **Statistics** menu from the Web UI.

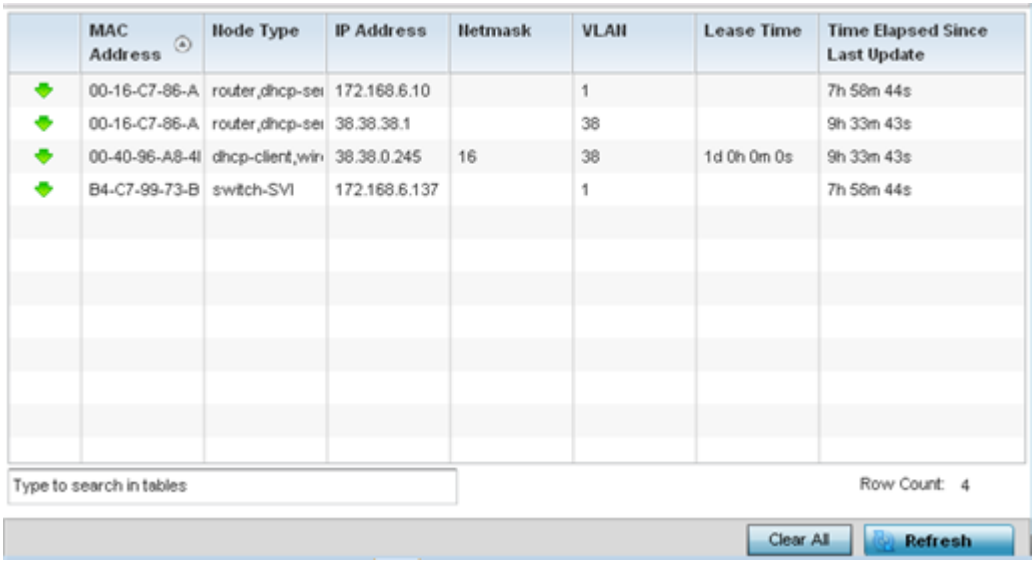
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **Firewall** menu.

5 Select **DHCP Snooping**.

The **Statistics > AP > Firewall > DHCP Snooping** screen displays in the right-hand pane.




This screen displays the following information:

| | |
|---|---|
| MAC Address | Displays the MAC address of the client requesting DHCP resources from the access point. |
| Node Type | Displays the NetBios node with an IP pool from which IP addresses can be issued to client requests on this interface. |
| IP Address | Displays the IP address used for DHCP discovery, and requests between the DHCP server and DHCP clients. |
| Netmask | Displays the subnet mask used for DHCP discovery, and requests between the DHCP server and DHCP clients. |
| VLAN | Displays the virtual interface used for a new DHCP configuration. |
| Lease Time | When a DHCP server allocates an address for a requesting DHCP client, the client is assigned a lease (which expires after a designated interval defined by the administrator). The lease is the time an IP address is reserved for re-connection after its last use. Using short leases, DHCP can dynamically reconfigure networks in which there are more computers than available IP addresses. This is useful, for example, in education and customer environments where client users change frequently. Use longer leases if there are fewer users. |
| Time Elapsed since Last Update | Displays the amount of time elapsed since the DHCP server was last updated. |

6 Select **Clear All** to revert the counters to zero and begin a new data collection.

7 Select **Refresh** to update the screen's counters to their latest values

*AP IPv6 Neighbor Snooping*

IPv6 snooping bundles layer 2 IPv6 hop security features, such as IPv6 ND inspection, IPv6 address gleaning and IPv6 device tracking. When IPv6 ND is configured on a device, packet capture instructions redirect the ND protocol and DHCP for IPv6 traffic up to the controller for inspection.

A database of connected IPv6 neighbors is created from the IPv6 neighbor snoop. The database is used by IPv6 to validate the link layer address, IPv6 address and prefix binding of the neighbors to prevent spoofing and potential redirect attacks.

Access Points listen to IPv6 formatted network traffic and forward IPv6 packets to radios on which the interested hosts are connected.

To review IPv6 neighbor snooping statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

The System node expands to display the RF Domains created within the managed network.

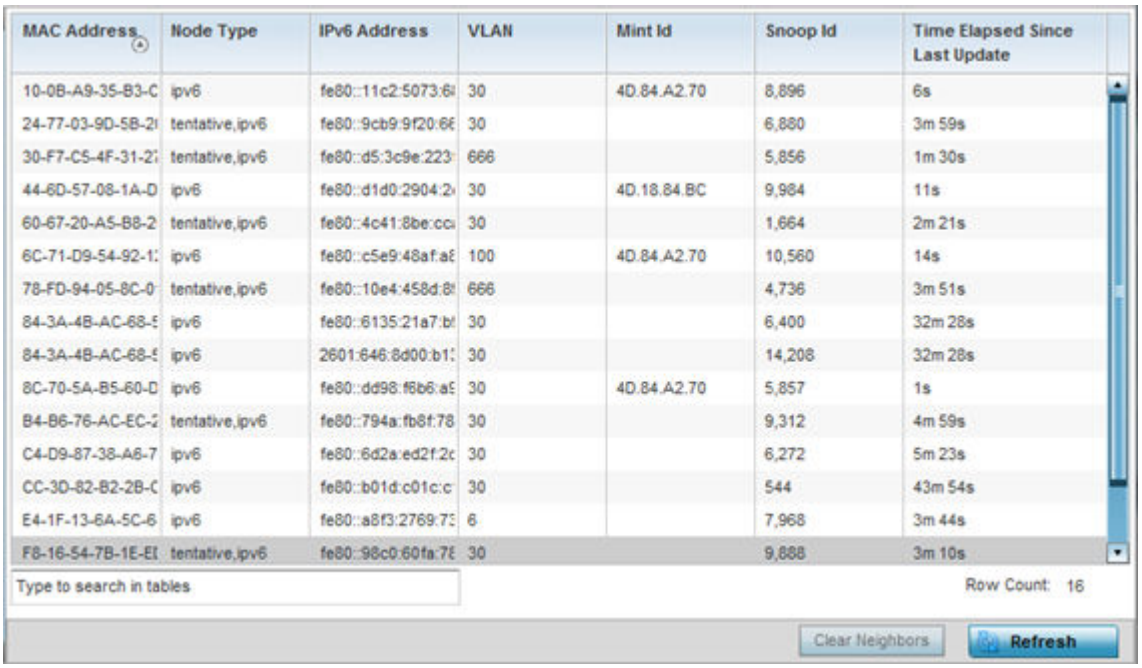
3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **Firewall** menu.

5 Select **IPv6 Neighbor Snooping**.

The **Statistics > AP > Firewall > IPv6 Neighbor Snooping** screen displays in the right-hand pane.




This screen displays the following information:

| | |
|---|---|
| MAC Address | Displays the hardware encoded MAC address of an IPv6 client reporting to the controller or service platform. |
| Node Type | Displays the NetBios node type from an IPv6 address pool from which IP addresses can be issued to requesting clients. |
| IPv6 Address | Displays the IPv6 address used for DHCPv6 discovery and requests between the DHCPv6 server and DHCP clients. |
| VLAN | Displays the controller or service platform virtual interface ID used for a new DHCPv6 configuration. |

| | |
|---|---|
| Mint Id | Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure communications at the transport layer. Using MiNT, a device can be configured to only communicate with other authorized (MiNT enabled) devices of the same model. |
| Snoop Id | Lists the numeric snooping session ID generated when Access Points listen to IPv6 formatted network traffic and forward IPv6 packets to radios. |
| Time Elapsed Since Last Update | Displays the amount of time elapsed since the DHCPv6 server was last updated. |

6 Select **Clear Neighbors** to revert the counters to zero and begin a new data collection.

7 Select **Refresh** to update the screen's counters to their latest values.

## AP VPN

IPsec VPN provides a secure tunnel between two networked peer access points. Administrators can define which packets are sent within the tunnel, and how they are protected. When a tunneled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the *inbound* and *outbound* direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Crypto maps combine the elements comprising IPsec SAs. Crypto maps also include *transform sets*. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

The IKE protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

VPN statistics are partitioned into the following:

- IKESA
- IPSec

### *AP VPN IKESA*

The **IKESA** screen allows for the review of individual peer security association statistics.

To view an access point's IKESA statistics:

1 Select the **Statistics** menu from the Web UI.

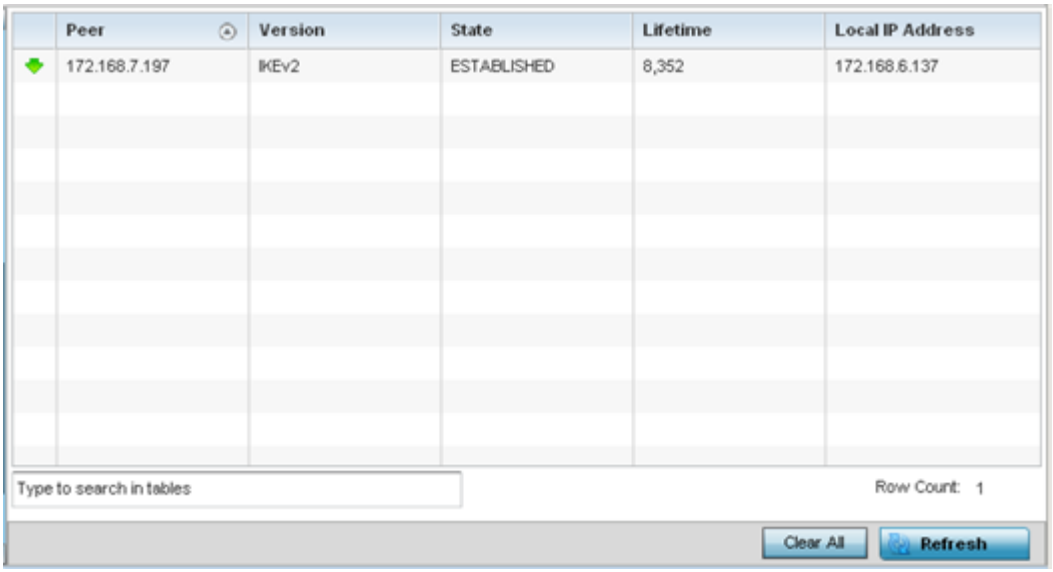
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **VPN** menu.

5 Select **IKESA**.

The **Statistics > AP > VPN > IKESA** screen displays in the right-hand pane.




Review the following VPN peer security association statistics:

| | |
|---|---|
| Peer | Lists peer IDs for peers sharing SA for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination. |
| Version | Displays each peer's IKE version used for auto IPSec secure authentication with the IPSec gateway and other controllers or service platforms. |
| State | Lists the state of each listed peer's SA (whether established or not). |
| Lifetime | Displays the lifetime for the duration of each listed peer IPSec VPN security association. Once the set value is exceeded, the association is timed out. |
| Local IP Address | Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address. |

6 Select a IKE peer configuration and click **Clear** to remove the peer from the table.

7 Select **Clear All** to clear each peer of its current status and begin a new data collection.

8 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP VPN IPSec*

To view an access point's IPSec VPN statistics:

1 Select the **Statistics** menu from the Web UI.

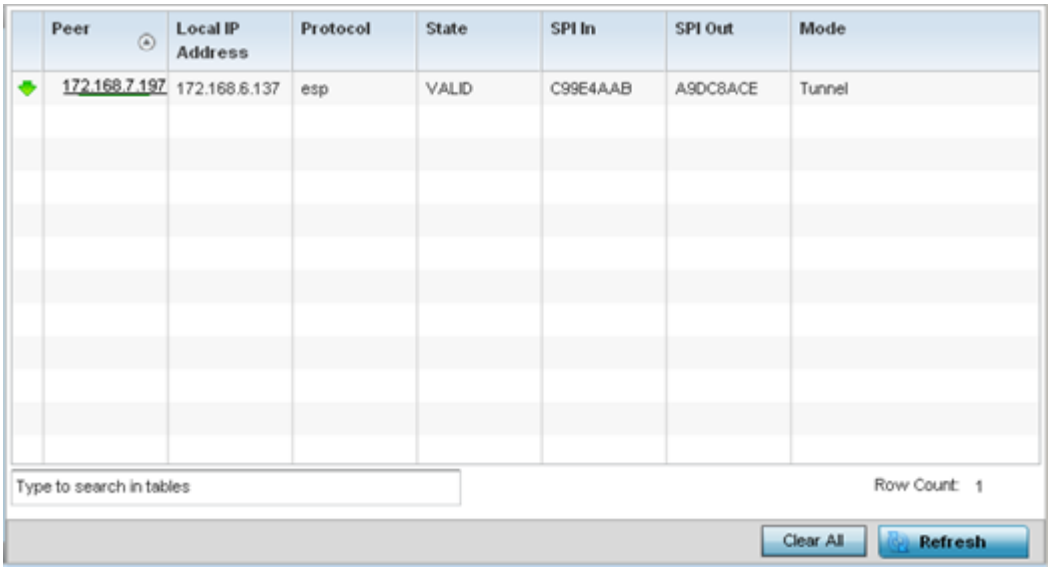
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **VPN** menu.

5 Select **IPSec**.

The **Statistics > AP > VPN > IPSec** screen displays in the right-hand pane.




Review the following VPN peer security association statistics:

| | |
|---|---|
| Peer | Lists IP addresses for peer IDs for peers sharing SAs for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination. |
| Local IP Address | Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address. |
| Protocol | Lists the security protocol used with the VPN IPSec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include **ESP** and **AH**. |
| State | Lists the state of each listed peer's security association. |
| SPI In | Lists SPI status for incoming IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid. |
| SPI Out | Lists SPI status for outgoing IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid. |
| Mode | Displays the IKE mode as either **Main** or **Aggressive**. IPSec has two modes in IKEv1 for key exchanges. The Aggressive mode requires three messages be exchanged between the IPSEC peers to setup the SA. The Main mode requires six messages. |

6 Select **Clear All** to clear each peer of its current status and begin a new data collection.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Certificates

The SSL protocol ensures secure transactions between Web servers and browsers. SSL uses a third-party CA to identify one (or both) ends of a transaction. A browser checks the certificate issued by the server before establishing a connection.

This screen is partitioned into the following:

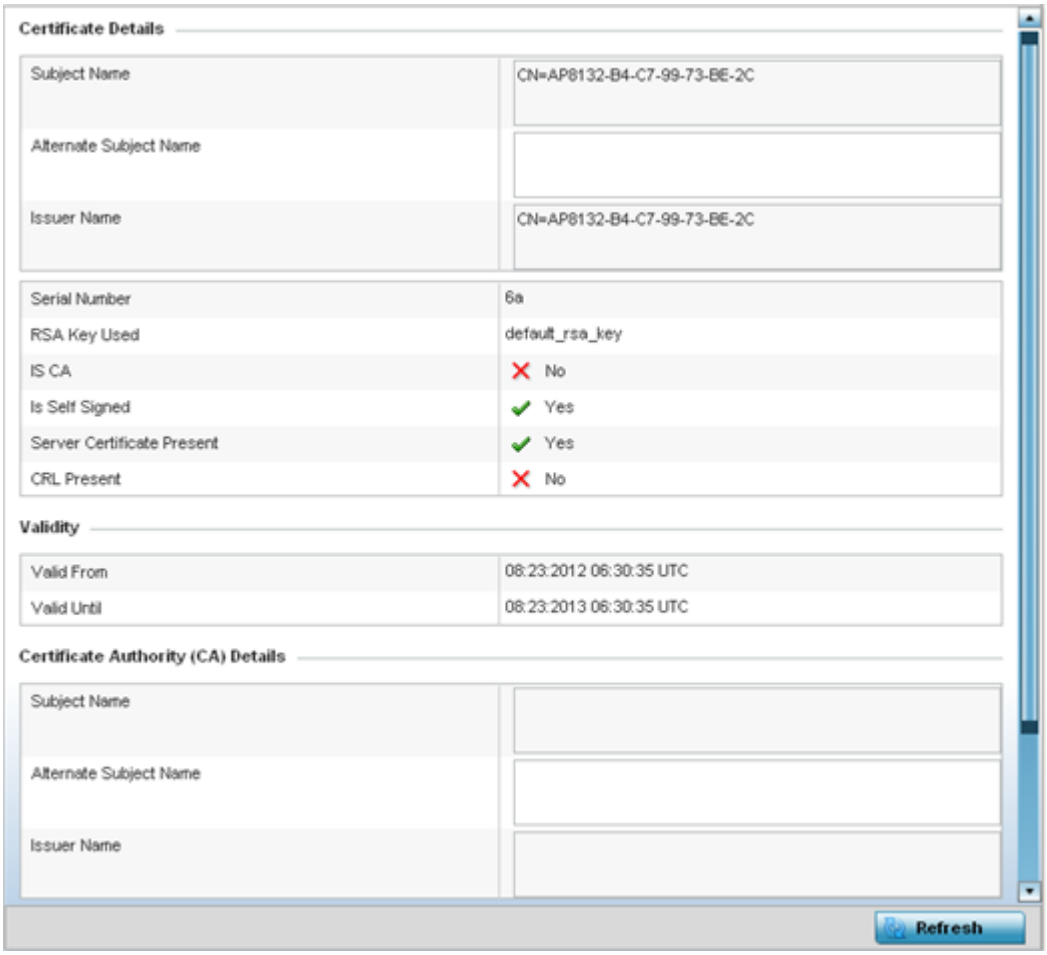
- AP Certificates Trustpoints on page 1074
- AP Certificates RSA Keys on page 1075

*AP Certificates Trustpoints*

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a *certificate authority*, *corporate* or *individual*. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **Certificates** menu.

The **Statistics > AP > Certificates > Trustpoints** screen displays by default right-hand pane.




The **Certificate Details** field displays the following:

| | |
|---|---|
| Subject Name | Describes the entity to which the certificate is issued. |
| Alternate Subject Name | Lists alternate subject information about the certificate as provided to the certificate authority. |
| Issuer Name | Displays the name of the organization issuing the certificate. |

| | |
|---|---|
| Serial Number | Lists the unique serial number of the certificate. |
| RSA Key Used | Displays the name of the key pair generated separated, or automatically when selecting a certificate. |
| IS CA | Indicates whether this certificate is an authority certificate (**Yes**/**No**). |
| Is Self Signed | Displays whether the certificate is self-signed (**Yes**/**No**). |
| Server Certification Present | Displays whether a server certification is present or not (**Yes**/**No**). |
| CRL Present | Displays whether a CRL is present (**Yes**/**No**). A CRL contains a list of subscribers paired with digital certificate status. The list displays revoked certificates along with the reasons for revocation. The date of issuance and the entities that issued the certificate are also included. |

The Validity field displays the following:

| | |
|---|---|
| Valid From | Displays the certificate's issue date. |
| Valid Until | Displays the certificate's expiration date. |

The **Certificate Authority (CA) Details** field displays the following:

| | |
|---|---|
| Subject Name | Displays information about the entity to which the certificate is issued. |
| Alternate Subject Name | This section provides alternate information about the certificate as provided to the certificate authority. This field is used to provide more information that supports information provided in the *Subject Name* field. |
| Issuer Name | Displays the organization issuing the certificate. |
| Serial Number | Lists the unique serial number of each certificate issued. |

The Certificate Authority Validity field displays the following:

| | |
|---|---|
| Validity From | Displays the date when the validity of a CA began. |
| Validity Until | Displays the date when the validity of a CA expires. |

Review the *Certificate Authority (CA) Details* and *Validity* information to assess the subject and certificate duration periods.

5 Periodically select the Refresh button to update the screen's statistics counters to their latest values.

### *AP Certificates RSA Keys*

RSA is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption.

The *RSA Keys* screen displays a list of RSA keys installed in the selected access point. RSA Keys are generally used for establishing a SSH session, and are a part of the certificate set used by RADIUS, VPN and HTTPS.

To view the access point's RSA Key details:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **Certificates** menu.
5 Select **RSA Keys**.

The **Statistics > AP > Certificates > RSA Keys** screen displays by default right-hand pane.


The RSA Key Details field describes the size (in bits) of the desired key. If not specified, a default key size of 1024 is used.

The RSA Public Key field describes the public key used for encrypting messages. This key is known to everyone.

6 Periodically select **Refresh** to update the screen's statistics counters to their latest values.

## AP WIPS

A WIPS monitors the wireless network's radio spectrum for the presence of unauthorized access points, and take measures to prevent an intrusion. Unauthorized attempts to access an access point managed WLAN is generally accompanied by anomalous behavior as intruding clients try to find network vulnerabilities. Basic forms of this behavior can be monitored and reported without a dedicated WIPS. When the parameters exceed a configurable threshold, a SNMP trap is generated that reports the results via management interfaces.

The WIPS screens provide details about blacklisted devices (unauthorized access points) intruding the network. Details include the name of the blacklisted client, the time when the client was blacklisted, the total time the client remained in the network, etc. The screen also provides WIPS event details.

For more information, see:

### *AP WIPS Client Blacklist*

The access point's **Client Blacklist** displays blacklisted clients detected by this access point using WIPS. Blacklisted clients are not allowed to associate to this access point.

To view the WIPS client blacklist for this access point:

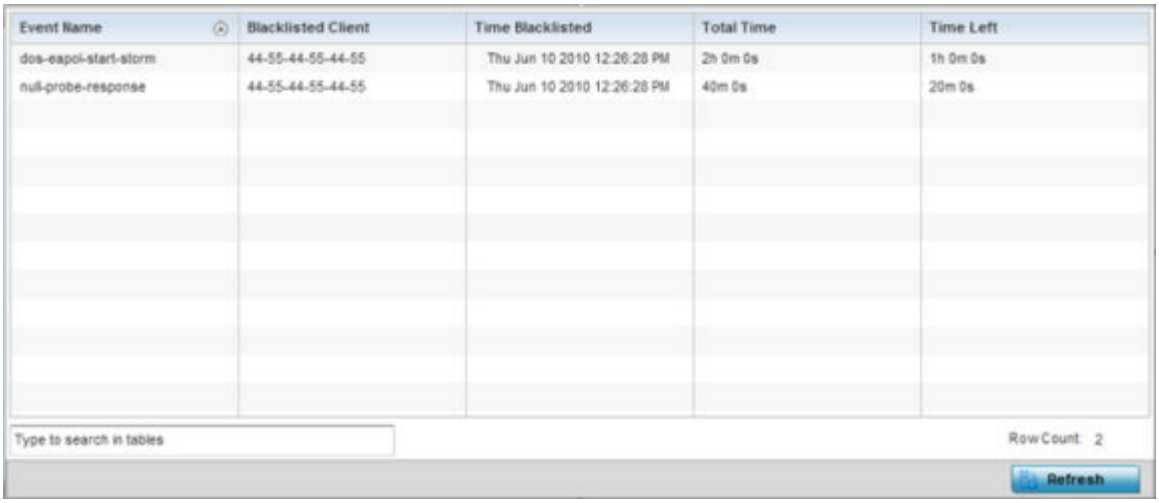
1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **WIPS** menu.

The **Statistics > AP > WIPS > Client Blacklist** screen displays by default right-hand pane




This screen displays the following:

| | |
|---|---|
| **Event Name** | Displays the name of the detected wireless intrusion resulting in a blacklisting of the client. |
| **Blacklisted Client** | Displays the MAC address of the unauthorized and blacklisted device intruding this access point's radio coverage area. |
| **Time Blacklisted** | Displays the time when the client was blacklisted by this access point. |
| **Total Time** | Displays the time the unauthorized (now blacklisted) device remained in this access point's WLAN. |
| **Time Left** | Displays the time the blacklisted client remains on the list. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

### *AP WIPS Events*

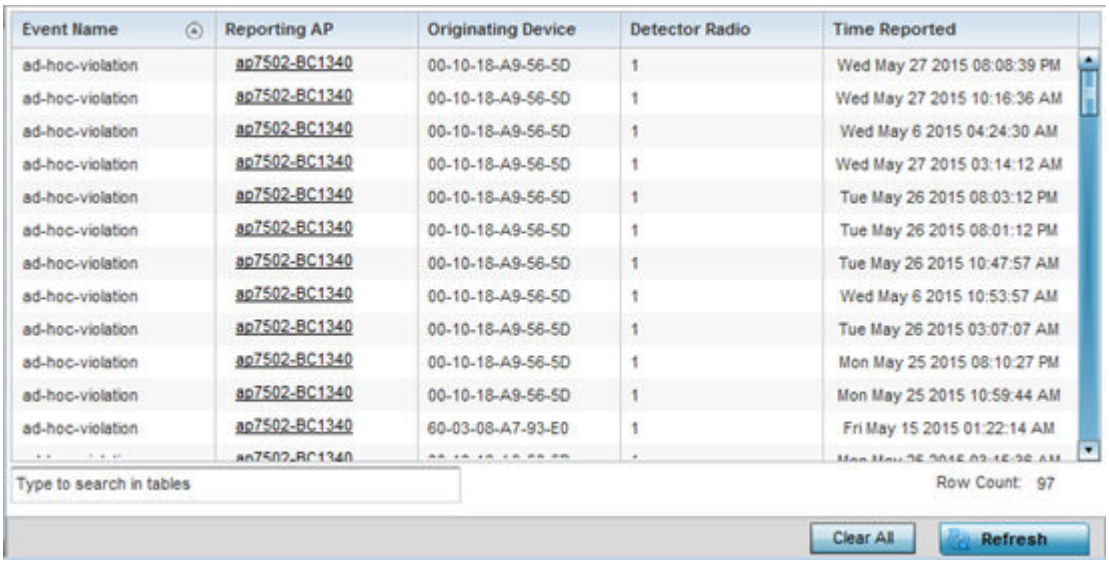
Periodically review the **WIPS Events** screen to assess whether any new or existing events require additional administration to protect the security of authorized devices. Events are listed by name,

detecting AP, originating device, detector radio and time. The reporting AP can be selected to review that AP's configuration in greater detail.

To view an access point's WIPS Events statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Expand the **WIPS** menu.
5 Select **WIPS Events**.

The **Statistics > AP > WIPS > WIPS Events** screen displays by default right-hand pane.




This screen displays the following information:

| | |
|---|---|
| Event Name | Displays the name of the detected wireless intrusion event. |
| Originating Device | Displays the MAC address of the intruder device. |
| Reporting AP | Displays the hostname of the AP reporting each intrusion. The access point displays as a link that can be selected to provide configuration and network address information in greater detail. |
| Detector Radio | Displays the number of the detecting access point radio. |
| Time Reported | Displays the time when the intrusion event was detected. |

6 Select **Clear All** to reset the statistics counters to zero and begin a new data collection.
7 Select **Refresh** to update the screen's statistics counters to their latest values.

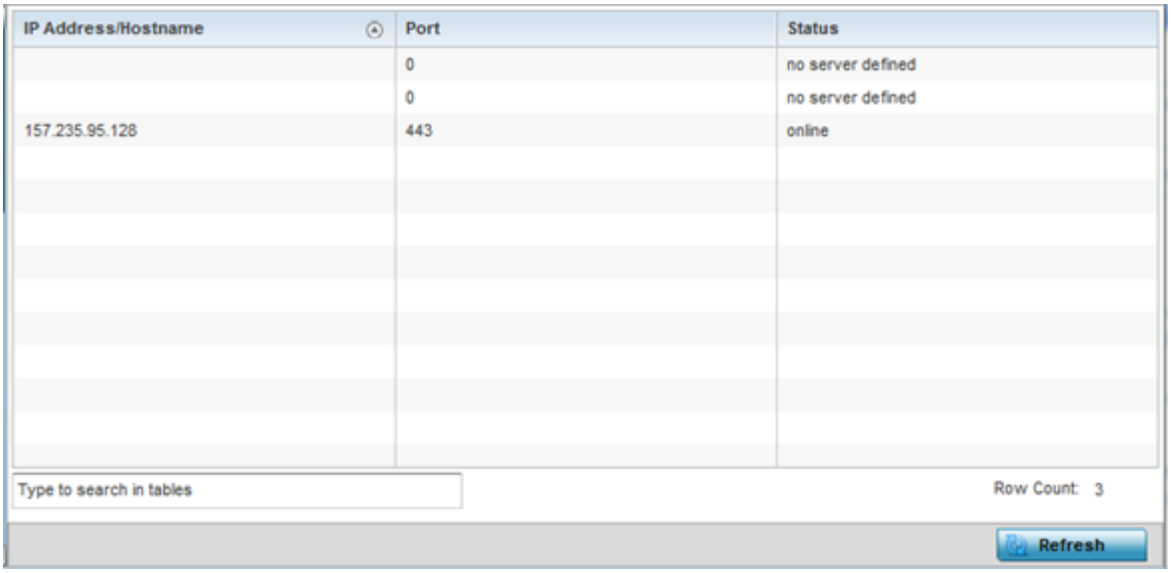
## AP Sensor Servers

Sensor Servers allow the monitor and download of data from multiple access points in sensor mode and remote locations using Ethernet TCP/IP or serial communication. Repeaters are available to extend the transmission range and combine sensors with various frequencies on the same receiver.

To view the network address and status information of the sensor server resources available to the access point:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **Sensor Servers**.

The **Statistics > AP > Sensor Servers** screen displays.




This screen displays the following:

| | |
|---|---|
| IP Address | Displays a list of sensor server IP addresses or administrator assigned hostnames. These are the server resources available to the access point for the management of data uploaded from dedicated sensors. |
| Port | Displays the numerical port where the sensor server is listening. Unconnected server resources are not able to provide sensor reporting. |
| Status | Displays whether the server is currently **`connected`** or **`not connected`**. |

5 Select **Refresh** to update the screen's statistics counters to their latest values

## AP Bonjour Services

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Zeroconf is a group of technologies including service discovery, address assignment and hostname resolution. Bonjour locates the devices (printers, computers, etc.) and services these computers provide over a local network.

Bonjour provides a method to discover services on a LAN. Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

To view the Bonjour service statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).

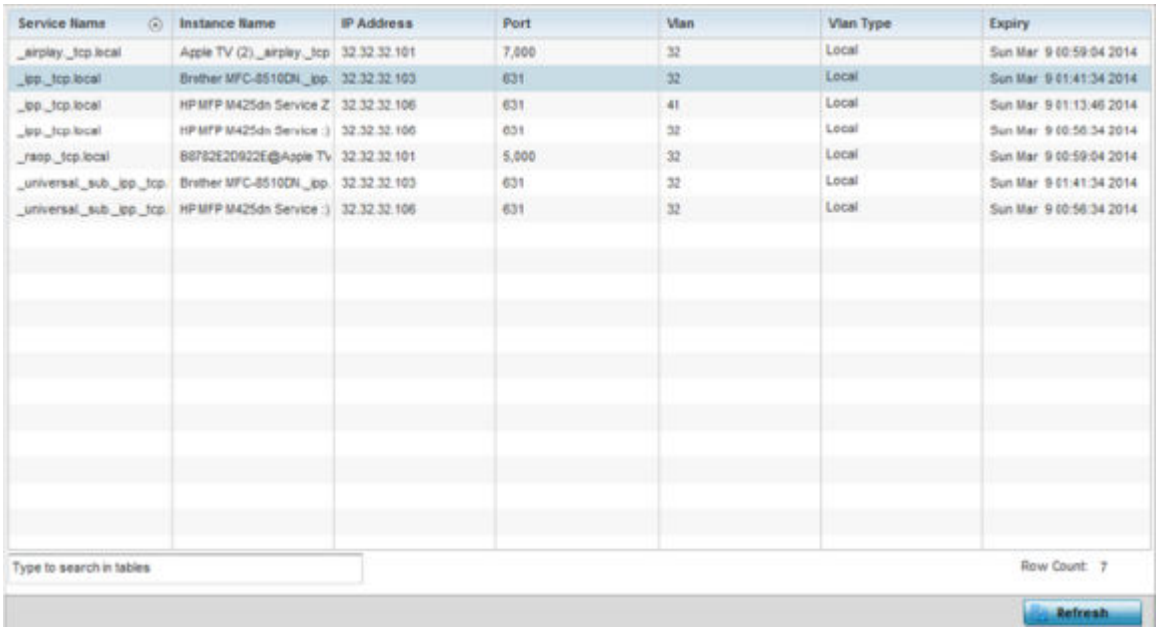
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points.

The Access Point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Select **Bonjour Services** from the left-hand side of the UI.

The **Statistics > AP > Bonjour Services** screen displays.




Refer to the following Bonjour service utilization stats:

| | |
|---|---|
| Service Name | Lists the services discoverable by the Bonjour gateway. Services can either be *pre-defined* Apple services (scanner, printer, etc.) or an alias not available on the predefined list. |
| Instance Name | Lists the name of each Bonjour service instance (session) utilized by the controller or service platform. |
| IP Address | Lists the network IP address utilized by the listed Bonjour service providing resources to the controller or service platform. |
| Port | Displays the port used to secure a connection with the listed Bonjour service. |
| Vlan | Lists the VLAN(s) on which a listed Bonjour service is routable. |
| Vlan Type | Lists the VLAN type as either a *local* bridging mode or a *shared tunnel*. |
| Expiry | Lists the expiration date of the listed Bonjour service, and its availability to discover resources on the LAN. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

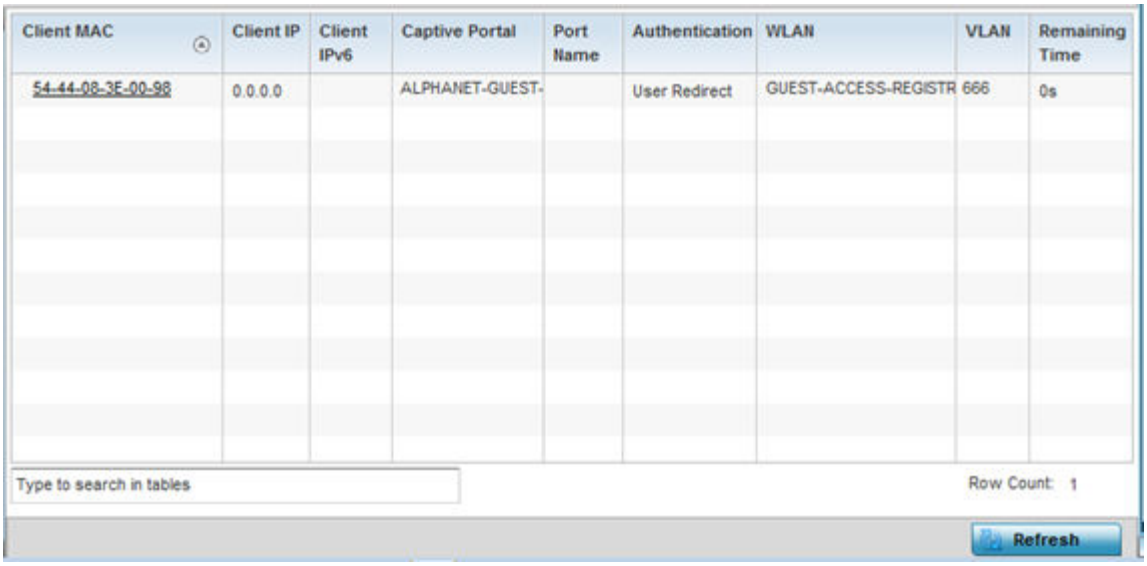
## AP Captive Portal

A *captive portal* forces HTTP clients, requesting network access, to use a special Web page for authentication before using the access point provisioned Internet. A captive portal turns a Web browser into a client authenticator. This is done by intercepting packets regardless of the address or port, until the user opens a browser and tries to access the Internet. At that time, the browser is redirected to a Web page.

To view an access point's captive portal statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select **Captive Portal**.

The **Statistics > AP > Captive Portal** screen displays.




This screen displays the following information:

| | |
|---|---|
| Client MAC | Displays the requesting client's MAC address. The MAC displays as a link that can be selected to display client configuration and network address information in greater detail. |
| Client IP | Displays the requesting client's IPv4 address. |
| Client IPv6 | Displays the requesting client's IPv6 formatted IP address. |
| Captive Portal | Displays the captive portal name that each listed client is utilizing for guest access to access point resources. |
| Port Name | Lists the access point port name supporting the captive portal connection with the listed client MAC address. |
| Authentication | Displays the authentication status of the requesting client. |
| WLAN | Displays the name of the WLAN utilizing the access point managed captive portal. |

| | |
|---|---|
| VLAN | Displays the name of the access point VLAN the requesting client uses as virtual interface for captive portal sessions. |
| Remaining Time | Displays the time after which the client is disconnected from the captive portal managed Internet. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Network Time

NTP *(Network Time Protocol)* is central to networks that rely on their controller or service platform to supply system time to managed devices. Without NTP, system time is unpredictable, which can result in data loss, failed processes and compromised security. With network speed, memory, and capability increasing at an exponential rate, the accuracy, precision, and synchronization of network time is essential in an enterprise network. The controller or service platform can optionally use a dedicated server to supply system time. The controller or service platform can also use several forms of NTP messaging to sync system time with authenticated network traffic.

The Network Time screen provides detailed statistics of an associated NTP Server of an access point. Use this screen to review the statistics for each access point.

The Network Time statistics screen consists of two tabs:

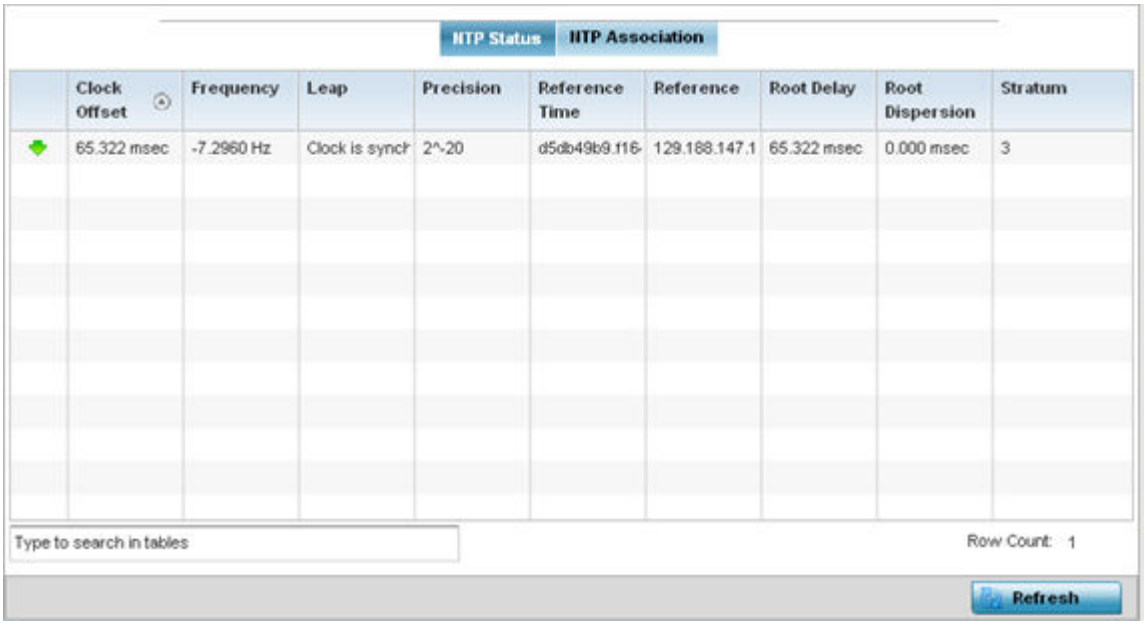
- AP NTP Status on page 1082
- AP NTP Association on page 1083

### *AP NTP Status*

To view an access point's NTP Status:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Expand the **Network Time** menu

The **Statistics > AP > Network Time > NTP Status** screen displays by default.




Use this screen to review the accuracy and performance of the synchronization with a NTP server resource.

| | |
|---|---|
| Clock Offset | Displays the time differential between the access point's time and its NTP resource's time. |
| Frequency | Indicates the SNTP server clock's skew (difference) for the access point. |
| Leap | Indicates if a second is added or subtracted to SNTP packet transmissions, or if transmissions are synchronized. |
| Precision | Displays the precision of the time clock (in Hz). The values that normally appear in this field range from -6, for mains-frequency clocks, to -20 for microsecond clocks. |
| Reference Time | Displays the time stamp the access point's clock was last synchronized or corrected. |
| Reference | Displays the address of the time source the access point is synchronized to. |
| Root Delay | The total round-trip delay in seconds. This variable can take on both positive and negative values, depending on relative time and frequency offsets. The values that normally appear in this field range from negative values (a few milliseconds) to positive values (several hundred milliseconds). |
| Root Dispersion | The difference between the time on the root NTP server and its reference clock. The reference clock is the clock used by the NTP server to set its own clock. |
| Stratum | Displays how many hops the access point is from its current NTP time resource. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

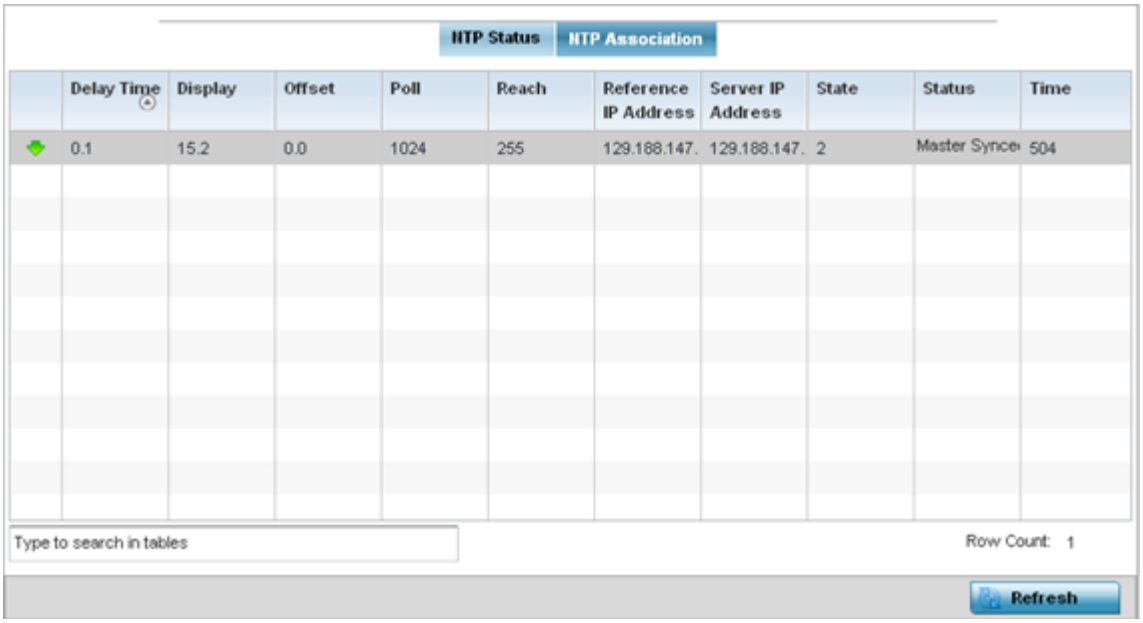
### *AP NTP Association*

The interaction between an access point and its dedicated external NTP server resource constitutes an *NTP Association*. NTP associations can be either *peer* associations (the access point synchronizes to another system or allows another system to synchronize to it), or *server* associations (only the access point synchronizes to the NTP resource, not the other way around).

To view the access point's NTP association statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
4 Select the **Network Time** menu.
5 Select the **NTP Association** tab.

The **Statistics > AP > Network Time > NTP Association** screen displays.




This screen displays the following:

| | |
|---|---|
| Delay Time | Displays the round-trip delay (in seconds) for broadcasts between the NTP server and the access point. |
| Display | Displays the time difference between the peer NTP server and the access point's clock. |
| Offset | Displays the calculated offset between the access point and the NTP server. The access point adjusts its clock to match the server's time value. The offset gravitates towards zero, but never completely reduces its offset to zero. |
| Poll | Displays the maximum interval between successive messages in seconds to the nearest power of two. |
| Reach | Displays the status of the last eight SNTP messages. If an SNTP packet is lost, the lost packet is tracked over the next eight SNTP messages. |
| Reference IP Address | Displays the address of the time source the access point is synchronized to. |
| Server IP Address | Displays the numerical IP address of the SNTP resource (server) providing SNTP updates to the access point. |

| | |
|---|---|
| State | Displays the NTP association status. This can be one of the following:<br>• **Synced** – Indicates the controller or service platform is synchronized to this NTP server.<br>• **Unsynced** – Indicates the controller or service platform has chosen this master for synchronization. However, the master itself is not yet synchronized to UTC.<br>• **Selected** – Indicates this NTP master server will be considered the next time the controller or service platform chooses a new master to synchronize with.<br>• **Candidate** – Indicates this NTP master server may be considered for selection the next time the controller or service platform chooses a NTP master server.<br>• **Configured** – Indicates this NTP server is a configured server. |
| Status | Displays how many hops the access point is from its current NTP time source. |
| Time | Displays the time of the last statistics update. |

6 Select **Refresh** to update the screen's statistics counters to their latest values

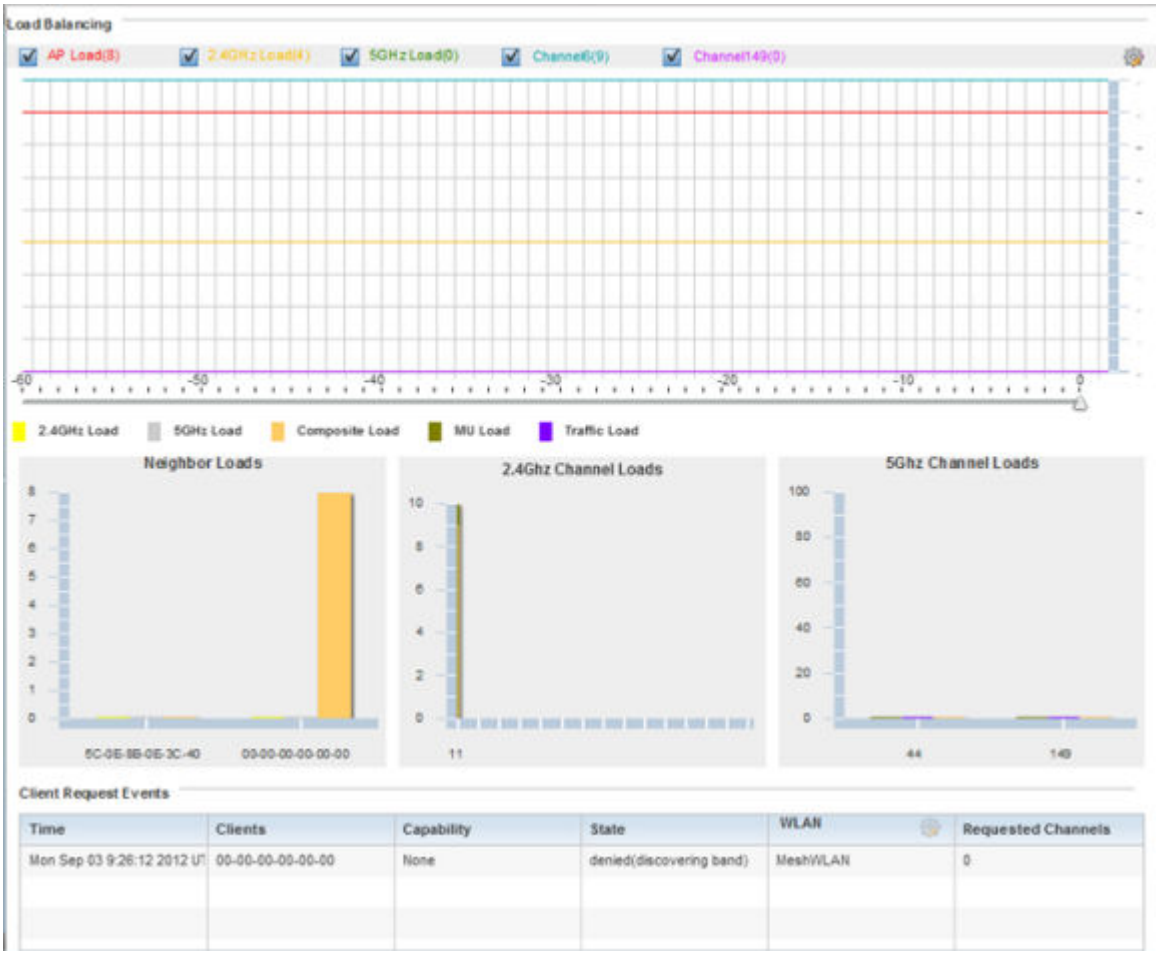
## AP Load Balancing

An access point's traffic load can be viewed graphically and filtered to display different load attributes. The access point's entire load can be displayed, as well as the separate loads on the 2.4 and 5 GHz radio bands. Operating channels can also be filtered. Each element can either be displayed individually or collectively in the graph.

To view the access point's load balance in a filtered graph format:

1 Select the Statistics menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4 Select **Load Balancing**.

The **Statistics > AP > Load Balancing** screen is displayed.




The **Load Balancing** screen displays the following:

| | |
|---|---|
| Load Balancing | Select any of the options to display any or all of the following information in the graph below: **`AP Load`**, **`2.4GHz Load`**, **`5GHz Load`**, and **`Channel.`** The graph section displays the load percentages for each of the selected variables over a period of time, which can be altered using the slider below the upper graph. |
| Client Requests Events | The Client Request Events displays the *Time*, *Client*, *Capability*, *State*, *WLAN* and *Requested Channels* for all client request events on the access point. All supported access point models support up to 256 clients per access point. |

5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Environment Statistics

An AP 8132 sensor module is a USB environmental sensor extension to an AP 8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the AP 8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

For more information, refer to the following:

- AP Light Sensor on page 1087.
- AP Temperature Sensor on page 1088.
- AP Motion Sensor on page 1089.
- AP Humidity Sensor on page 1090,

*AP Light Sensor*

To view an AP 8132 model access point's environmental light statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Select **Environment**. The **Statistics > AP 8132 > Environment > Light** tab displays by default.

Additional **Temperature**, **Motion** and **Humidity** tabs available for unique sensor reporting. Each of these sensor measurements helps the administrator determine whether the AP 8132's immediate deployment area is occupied by changes in the access point's environment.


5 Refer to the **Light** table to assess the sensor's detected light intensity within the AP 8132 immediate deployment area.

Light intensity is measured by the sensor in lumens. The table displays the **Current Light Intensity (lumens)** and the **20 Minute Average of Light Intensity (lumens)**. Compare these two items to determine whether the AP 8132's deployment location remains consistently lit, as an administrator can power off the access point's radios when no activity is detected in the immediate deployment area.

6 Refer to the Light Intensity Trend Over Last Hour graph to assess the fluctuation in lighting over the last hour. Use this graph to assess the deployment areas light intensity of particular hours of the day as needed to conjunction with the daily graph immediately below it.

7 Refer to the Light Intensity Trend Over Last Day graph to assess whether lighting is consistent across specific hours of the day. Use this information to help determine whether the AP 8132 can be upgraded or powered off during specific hours of the day.

8 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

*AP Temperature Sensor*

To view an AP 8132 model access point's environmental temperature:

1 Select the Statistics menu from the Web UI.

2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **Environment** menu.

5 Select the **Temperature** tab.

The Statistics > AP 8132 > Environment > Temperature tab displays.


6 Refer to the Temperature table to assess the sensor's detected temperature within the AP 8132's immediate deployment area.

Temperature is measured in centigrade. The table displays the Current Temperature (centigrade) and the 20 Minute Average Temperature (centigrade). Compare these two items to determine whether the AP 8132's deployment location remains consistently heated.

7 Refer to the Temperature Trend Over Last Hour graph to assess the fluctuation in ambient temperature over the last hour. Use this graph in combination with the Light and Motions graphs (in particular) to assess the deployment area's activity level.

8 Refer to the **Temperature Trend Over Last Day** graph to assess whether deployment area temperature is consistent across specific hours of the day. Use this information to help determine whether the AP 8132 can be upgraded or powered off during specific hours of the day.

9 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

*AP Motion Sensor*

To view an AP 8132 model access point's deployment area motion activity:

1 Select the **Statistics** menu from the Web UI.

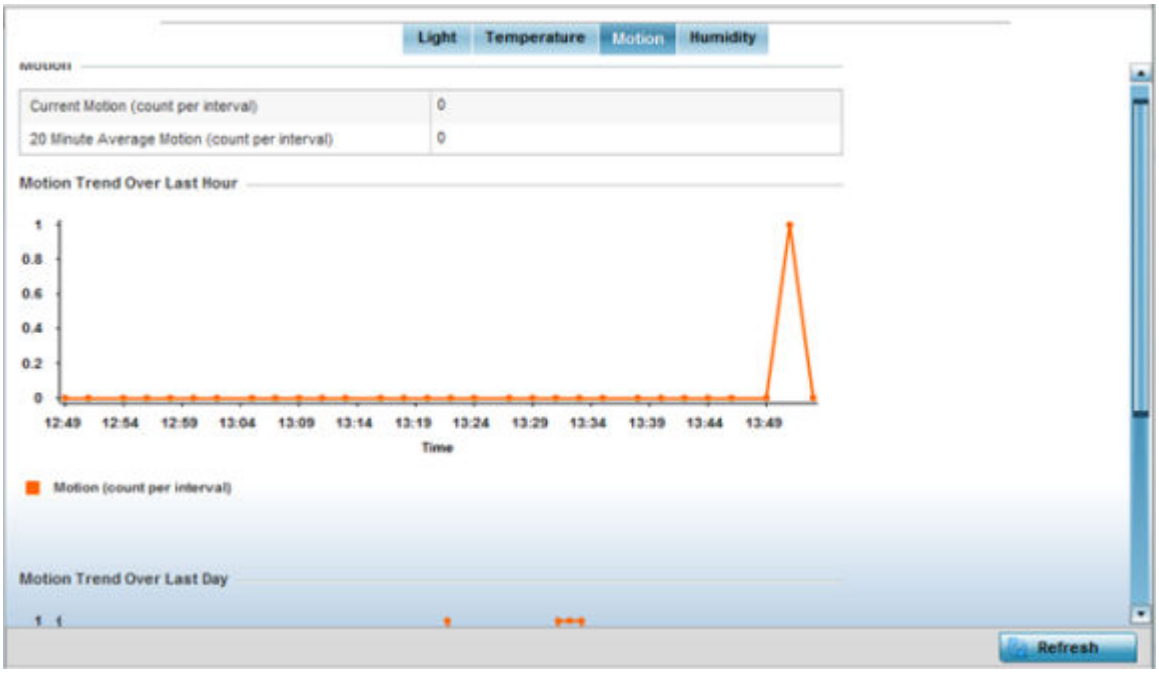
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **Environment** menu.

5 Select the **Motion** tab.

The **Statistics > AP 8132 > Environment > Motion** tab displays.




6 Refer to the **Motion** table to assess the sensor's detected movement within the AP 8132's immediate deployment area.

Motion is measured in intervals. The table displays the **Current Motion (count per interval)** and the **20 Minute Average Motion (count per interval)**. Compare these two items to determine whether the AP 8132's deployment location remains consistently occupied by client users.

7 Refer to the **Motion Trend Over Last Hour** graph to assess the fluctuation in user movement over the last hour. Use this graph in combination with the Light and Temperature graphs (in particular) to assess the deployment area's activity level.

8 Refer to the **Motion Trend Over Last Day** graph to assess whether deployment area user movement is consistent across specific hours of the day. Use this information to help determine whether the AP 8132 can be upgraded or powered off during specific hours of the day.

9 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

*AP Humidity Sensor*

To view an AP 8132 model access point's deployment area humidity:

1 Select the **Statistics** menu from the Web UI.

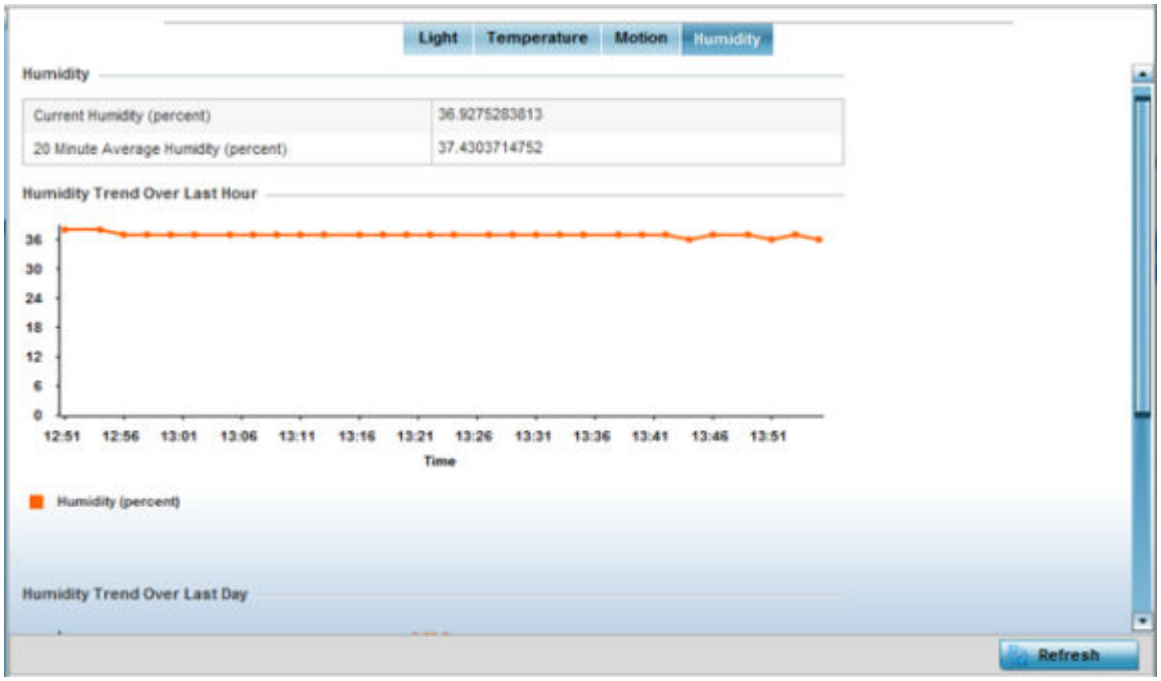
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, and select one of it's connected access points. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

4 Expand the **Environment** menu.

5 Select the **Humidity** tab.

The **Statistics > AP 8132 > Environment > Humidity** tab displays.




6 Refer to the **Humidity** table to assess the sensor's detected humidity fluctuations within the AP 8132's immediate deployment area.

Humidity is measured in percentage. The table displays the **Current Humidity (percent)** and the **20 Minute Average Humidity (percent)**. Compare these two items to determine whether the AP 8132's deployment location remains consistently humid (often a by-product of temperature).

7 Refer to the **Humidity Trend Over Last Hour** graph to assess the fluctuation in humidity over the last hour. Use this graph in combination with the Temperature and Motions graphs (in particular) to assess the deployment area's activity levels.

8 Refer to the **Humidity Trend Over Last Day** graph to assess whether deployment area humidity is consistent across specific hours of the day. Use this information to help determine whether the AP 8132 can be upgraded or powered off during specific hours of the day.

9 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

## AP IOT Imagotag

The WiNG AP-8432 model access points support SES-imagotag's ESL tags. An Imagotag-enabled AP recognizes the ESL communicator and facilitates communication between communicator and tags. To enable an AP-8432 as an infrastructure device facilitating communication between the ESL communicator and tags, an Imagotag policy is applied either to the AP's self (standalone AP) or to the AP's profile (adopted AP). Use this option to view the configuration of the ESL communicator.

**Note**
For information on enabling IOT Imagotag on an AP-8432, see Setting the Imagotag Policy on page 845

To view an AP-8432 model access point's ESL communicator configuration:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller or service platform, and select one of its connected AP-8432 access point.

3 Select **IOT Imagotag** from the AP's statistics menu.

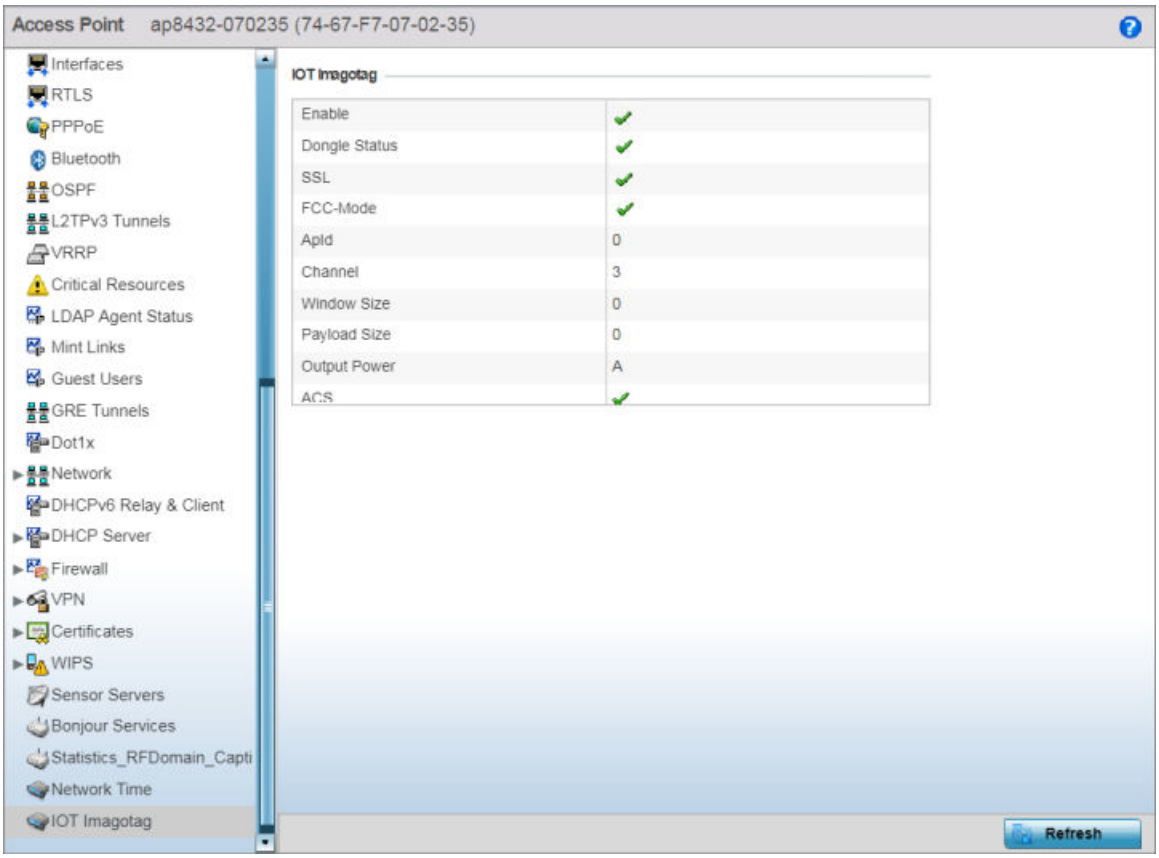



**Figure 430: Statistics → Access Point → IOT Imagotag screen**

4 Review the following IOT Imagotag details:

| | |
|---|---|
| Enable | Displays the status of the policy: Enabled/Disabled. A green check mark indicates that the policy is enabled. A red cross mark indicates that the policy is disabled. |
| Dongle Status | Displays the ESL communicator (USB Dongle) status - Connected/ Disconnected. |
| SSL | Displays if SSL *(Secure Socket Layer)* encryption mode of communication is enabled or not. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled. |
| FCC-Mode | Displays if FCC compatibility mode is enabled or not on the ESL communicator. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled. |
| ApId | Displays the Imagotag enabled AP's ID. |
| Channel | Displays the channel assigned for ESL communicator to tag communication in the 2.4 GHz band. |
| Window Size | Displays the transmission window size set for messages exchanged between ESL communicator and tags. |
| Payload Size | Displays the maximum payload size in packets exchanged between ESL communicator and tags. |

| | |
|---|---|
| Output Power | Displays the maximum output power set for the ESL communicator. |
| ACS | Displays if ACS *(Auto-Channel Selection)* status - Enabled/Disabled. |

# Wireless Client Statistics

Wireless Client statistics display read-only stats for a client selected from its connected access point, controller or service platform topology. Client stats help administrate client performance within an access point, controller or service platform managed network. Use this information to assess if configuration changes are required to improve client throughput.

Wireless client stats can be administrated using the following:

- Client Health on page 1093.
- Client Details on page 1096.
- Client Traffic on page 1099.
- Client WMM TSPEC on page 1102.
- Client Association History on page 1103.
- Client Graph on page 1104.

## Client Health

The Health screen displays performance information of a selected wireless client, in respect to the client's connected access point radio and managing controller, service platform or access point.

To view the health of a wireless client:

1 Select the **Statistics** menu from the Web UI.
2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller, an access point, then a connected client.
3 Select **Health**.

The **Statistics > Wireless Client > Health** screen displays by default.

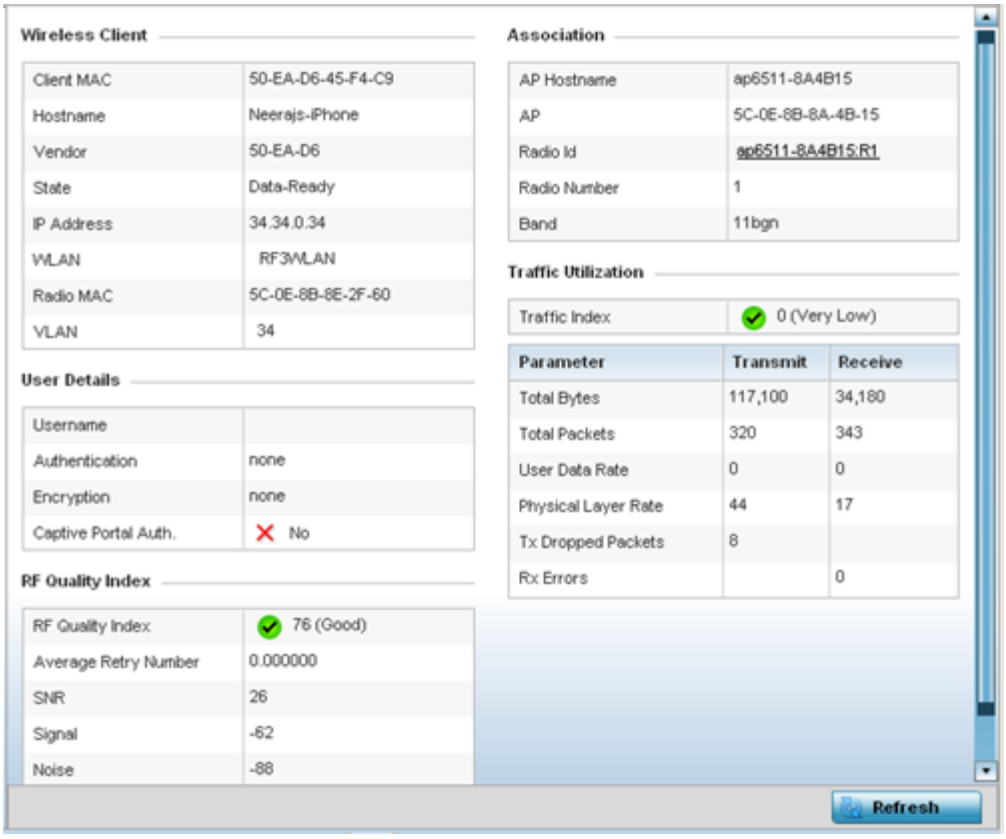



**Figure 431: Wireless Client - Statistics - Health Screen**

Refer the tables below for wireless client related data.

The Wireless Client field displays the following:

| | |
|---|---|
| Client MAC | Displays the factory encoded MAC address of the selected wireless client. |
| Hostname | Lists the hostname assigned to the client when initially managed by the controller, service platform or access point. |
| Vendor | Displays the vendor name (manufacturer) of the wireless client. |
| State | Displays the current operational state of the wireless client. The client's state can be **idle**, **authenticated**, **roaming**, **associated** or **blacklisted**. |
| IP Address | Displays the IP address the selected wireless client is currently utilizing as a network identifier. |
| WLAN | Displays the client's connected access point WLAN membership. This is the WLAN whose QoS settings should account for the client's radio traffic objective. |
| Radio MAC | Displays the access point radio MAC address the wireless client is connected to on the network. |
| VLAN | Displays the VLAN ID the access point has defined for use as a virtual interface with the client. |

The User Details field displays the following:

| | |
|---|---|
| Username | Displays the unique name of the administrator or operator supporting the client's managing controller, service platform or access point. |
| Authentication | Lists the authentication scheme applied to the client for interoperation with the access point. |
| Encryption | Lists the encryption scheme applied to the client for interoperation with the access point. |
| Captive Portal Authentication | Displays whether captive portal authentication is enabled for the client as a guest access medium to the controller or service platform managed network. |

The RF Quality Index field displays the following:

| | |
|---|---|
| RF Quality Index | Displays information on the RF quality for the selected wireless client. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions, as well as the retry and error rate. RF quality index can be interpreted as:<br>• *0 – 20* (Very poor quality)<br>• *20 – 40* (Poor quality)<br>• *40 – 60* (Average quality)<br>• *60 – 100* (Good quality) |
| Retry Rate | Displays the average number of retries per packet. A high number indicates possible network or hardware problems. |
| SNR | Displays the SNR ratio of the connected wireless client. |
| Signal | Displays the power of the radio signals in - dBm. |
| Noise | Displays the disturbing influences on the signal by interference of signals in - dBm. |
| Error Rate | Displays the number of received bit rates altered due to noise, interference and distortion. It is a unit-less performance measure. |

The Association field displays the following:

| | |
|---|---|
| AP Hostname | Lists the administrator assigned device name of the client's connected access point. |
| AP | Displays the MAC address of the client's connected access point. |
| Radio | Lists the target access point that houses the radio. Select the access point to view performance information in greater detail. |
| Radio ID | Lists the hardware encoded MAC address the radio uses as a hardware identifier that further distinguishes the radio from others within the same device. |
| Radio Number | Displays the access point's radio number (either 1, 2 or 3) to which the selected client is associated. |
| Radio Type | Displays the radio type. The radio can be *802.11b*, *802.11bg*, *802.11bgn*, *802.11a* or *802.11an*. |

The Traffic Utilization field displays statistics on the traffic generated and received by the selected client. This area displays the traffic index, which measures how efficiently the traffic medium is utilized. It's defined as the percentage of current throughput relative to the maximum possible throughput.

Traffic indices are:

- *0 – 20* (Very low utilization)
- *20 – 40* (Low utilization)

- *40 – 60* (Moderate utilization)
- *60 and above* (High utilization)

This table displays the following:

| | |
|---|---|
| Total Bytes | Displays the total bytes processed by the access point's connected wireless client. |
| Total Packets | Displays the total number of packets processed by the wireless client. |
| User Data Rate | Displays the average user data rate in both directions. |
| Physical Layer Rate | Displays the average packet rate at the physical layer in both directions. |
| Tx Dropped Packets | Displays the number of packets dropped during transmission. |
| Rx Errors | Displays the number of errors encountered during data transmission. The higher the error rate, the less reliable the connection or data transfer between the client and connected access point. |

4 Select **Refresh** to update the screen's statistics counters to their latest values.

## Client Details

The **Details** screen provides granular performance, network address, connection and association information for a selected wireless client.

To view the details screen of a connected wireless client:

1 Select the **Statistics** menu from the Web UI.
2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller, an access point, then a connected client.
3 Select **Details**.

The **Statistics > Wireless Client > Details** screen is displayed.

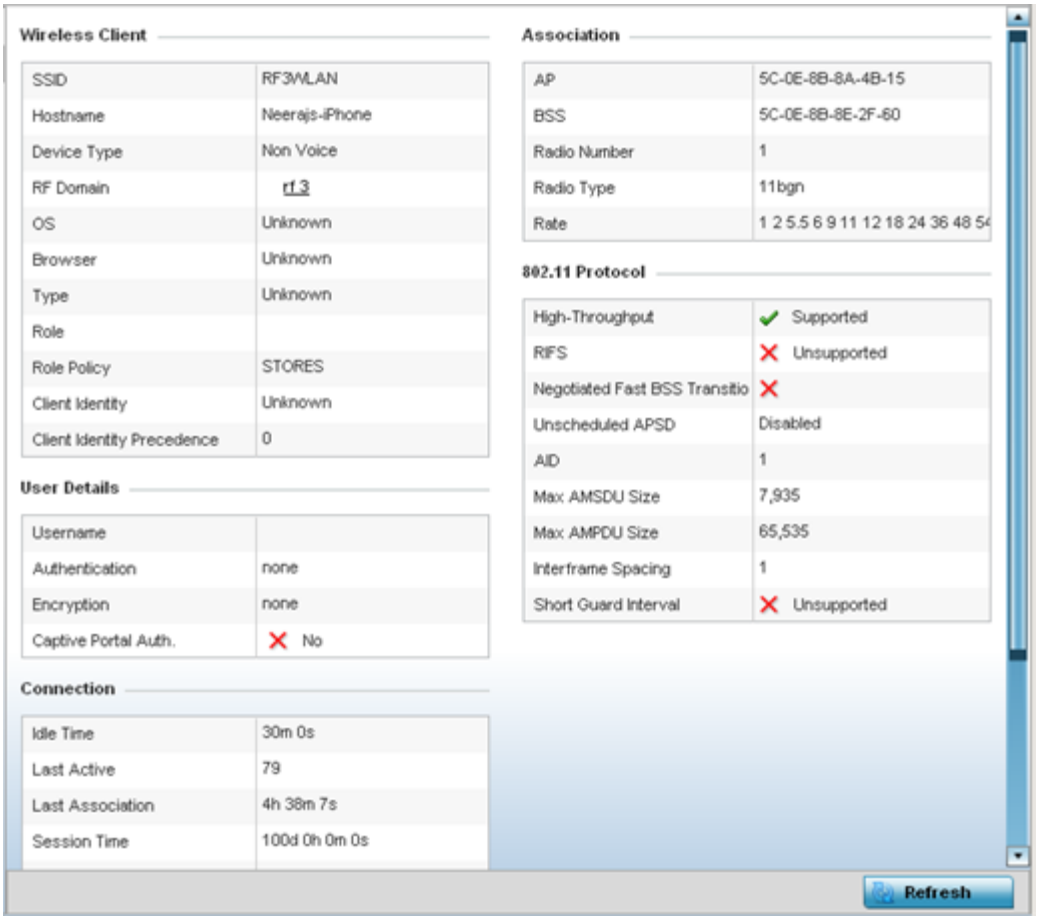



**Figure 432: Wireless Client Detailed Statistics Screen**

The Wireless Client field displays the following:

| | |
|---|---|
| SSID | Displays the client's SSID. |
| Hostname | Lists the hostname assigned to the client when initially managed by the controller, service platform or access point managed network. |
| Device Type | Displays the client device type providing the details to the operating system. |
| RF Domain | Displays the RF Domain to which the connected client is a member via its connected access point, controller or service platform. The RF Domain displays as a link that can be selected to display RF Domain member, configuration and network address information in greater detail. |
| OS | Lists the client's operating system (Android, etc.). |
| Browser | Displays the browser type used by the client to facilitate its wireless connection. |
| Type | Lists the client manufacturer (or vendor). |
| Role | Lists the client's defined role in the controller, service platform or access point managed network. |
| Role Policy | Lists the user role set for the client as it became a controller, service platform or access point managed device. |

| | |
|---|---|
| Client Identity | Displays the unique vendor identity (Android, Windows, etc.) of the listed device as it appears to its adopting controller or service platform. |
| Client Identity Precedence | Lists the numeric precedence this client uses in establishing its identity amongst its peers. |
| Protected Management Frames | A green checkmark defines management frames as protected between this client and its associated access point radio. A red X states that management frames are disabled for the client and its connected radio. |
| Transmit Power Management | Lists the number power management frames exchanged between this client and its connected access point radio. Lists zero when disabled. |

The User Details field displays the following:

| | |
|---|---|
| Username | Displays the unique name of the administrator or operator managing the client's connected access point, controller or service platform. |
| Authentication | Lists the authentication scheme applied to the client for interoperation with its connected access point radio. |
| Encryption | Lists the encryption scheme applied to the client for interoperation with its connected access point radio. |
| Captive Portal Auth. | Displays whether captive portal authentication is enabled. When enabled, a restrictive set of access permissions may be in effect. |

The Connection field displays the following:

| | |
|---|---|
| Idle Time | Displays the time for which the wireless client remained idle. |
| Last Active | Displays the time in seconds the wireless client was last interoperating with its connected access point. |
| Last Association | Displays the duration the wireless client was in association with its connected access point. |
| Session Time | Displays the duration for which a session can be maintained by the wireless client without it being dis-associated from its connected access point radio. |
| SM Power Save Mode | Displays whether this feature is enabled on the wireless client. The SM *(spatial multiplexing)* power save mode allows an 802.11n client to power down all but one of its radios. This power save mode has two sub modes of operation: **`static operation`** and **`dynamic operation`**. |
| Power Save Mode | Displays whether this feature is enabled or not. To prolong battery life, the 802.11 standard defines an optional *Power Save Mode*, which is available on most 80211 clients. End users can simply turn it on or off via the card driver or configuration tool. With power save off, the 802.11 network card is generally in receive mode listening for packets and occasionally in transmit mode when sending packets. These modes require the 802.11 NIC to keep most circuits powered-up and ready for operation. |
| WMM Support | Displays whether WMM is enabled or not in order to provide data packet type prioritization between the access point and connected client. |
| 40 MHz Capable | Displays whether the wireless client has 802.11n channels operating at 40 MHz. |
| Max Physical Rate | Displays the client's maximum data rate at the physical layer. |
| Max User Rate | Displays the maximum client's permitted user data rate. |
| MC2UC Streams | Lists the number or multicast to unicast data streams detected. |

The **Association** field displays the following:

| | |
|---|---|
| AP | Displays the MAC address of the wireless client's connected access point. |
| BSS | Displays the BSS *(Basic Service Set)* the access point belongs to. A BSS is a set of stations that can communicate with one another. |
| Radio Number | Displays the access point radio number the wireless client is connected to. |
| Radio Type | Displays the radio type. The radio can be **802.11b**, **802.11bg**, **802.11bgn**, **802.11a** or **802.11an**. |
| Rate | Displays the permitted data rate for controller managed access point and client interoperation. |

The **802.11 Protocol** field displays the following:

| | |
|---|---|
| High-Throughput | Displays whether high throughput is supported. High throughput is a measure of successful packet delivery over a communication channel. |
| RIFS | Displays whether RIFS is supported. RIFS is a required 802.11n feature that improves performance by reducing the amount of dead time between OFDM transmissions. |
| Negotiated Fast BSS Transition | Lists whether Fast BSS transition is negotiated. This indicates support for a seamless fast and secure client handoff between two access points, controllers or service platforms. |
| Unscheduled APSD | Displays whether APSD is supported. APSD defines an unscheduled service period, which is a contiguous period of time during which the access point is expected to be awake. |
| AID | Displays the AID *(Association ID)* established by an AP. 802.11 association enables the access point to allocate resources and synchronize with a client. A client begins the association process by sending an association request to an access point. This association request is sent as a frame. This frame carries information about the client and the SSID of the network it wishes to associate. After receiving the request, the access point considers associating with the client, and reserves memory space for establishing an AID for the client. |
| Max AMSDU Size | Displays the maximum size of AMSDU. AMSDU is a set of Ethernet frames to the same destination that are wrapped in a 802.11n frame. This values is the maximum AMSDU frame size in bytes. |
| Max AMPDU Size | Displays the maximum size of AMPDU. AMPDU is a set of Ethernet frames to the same destination wrapped in an 802.11n MAC header. AMPDUs are used in noisy environments to provide reliable packet transmission. This value is the maximum AMPDU size in bytes. |
| Interframe Spacing | Displays the time interval between two consecutive Ethernet frames. |
| Short Guard Interval | Displays the guard interval in micro seconds. Guard intervals prevent interference between data transmissions. The guard interval is the space between characters being transmitted. The guard interval eliminates ISI *(inter-symbol interference)*. ISI occurs when echoes or reflections from one character interfere with another character. Adding time between transmissions allows echo's and reflections to settle before the next character is transmitted. A shorter guard interval results in shorter character times which reduces overhead and increases data rates by up to 10%. |

4 Select **Refresh** to update the screen's statistics counters to their latest values.

## Client Traffic

The **Traffic** screen provides an overview of client traffic utilization in both the transmit and receive directions. This screen also displays a RF quality index.

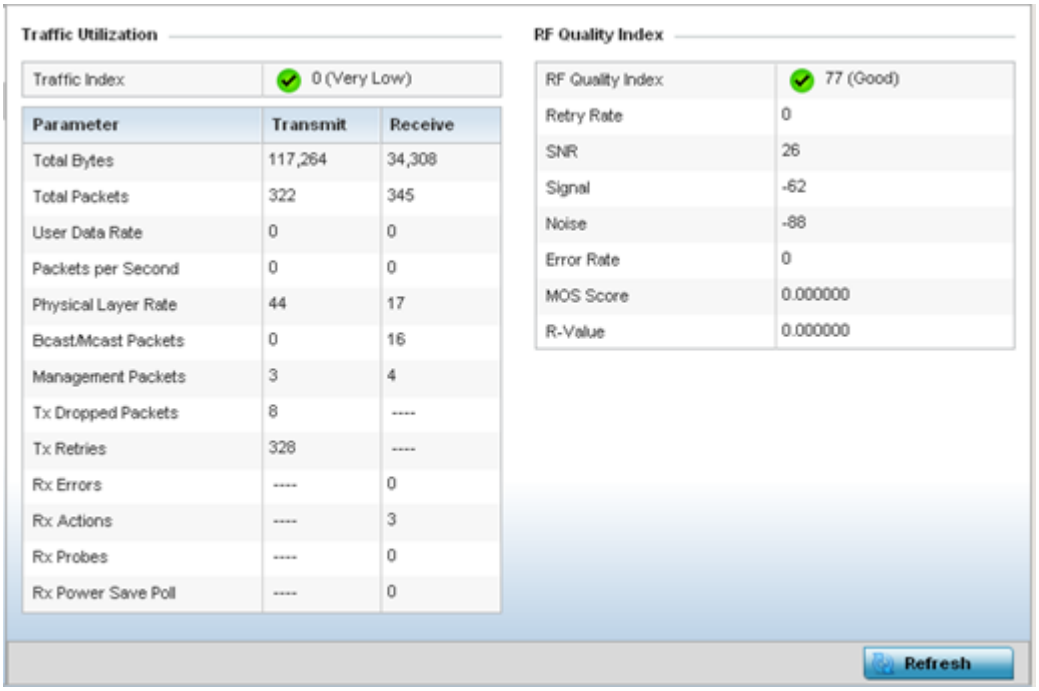
To view the traffic statistics of a wireless clients:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller, an access point, then a connected client.

3 Select **Traffic**.

The **Statistics > Wireless Client > Traffic** screen is displayed.




The Traffic Utilization statistics employs an index, which measures how efficiently the traffic medium is used. It's defined as the percentage of current throughput relative to the maximum possible throughput. The traffic indices are:

- *0 – 20* (Very low utilization)
- *20 – 40* (Low utilization)
- *40 – 60* (Moderate utilization)
- *60 and above* (High utilization)

This screen also provides the following:

| | |
|---|---|
| Total Bytes | Displays the total bytes processed (in both directions) by the access point's connected client. |
| Total Packets | Displays the total number of data packets processed (in both directions) by the access point's connected wireless client. |
| User Data Rate | Displays the average user data rate. |
| Packets per Second | Displays the packets processed per second. |
| Physical Layer Rate | Displays the data rate at the physical layer level. |
| Bcast/Mcast Packets | Displays the total number of broadcast/management packets processed by the client. |
| Management Packets | Displays the number of management (overhead) packets processed by the client. |

| | |
|---|---|
| Tx Dropped Packets | Displays the client's number of dropped packets while transmitting to its connected access point. |
| Tx Retries | Displays the total number of client transmit retries with its connected access point. |
| Rx Errors | Displays the errors encountered by the client during data transmission. The higher the error rate, the less reliable the connection or data transfer between client and connected access point. |
| Rx Actions | Displays the number of receive actions during data transmission with the client's connected access point. |
| Rx Probes | Displays the number of probes sent. A probe is a program or other device inserted at a key juncture in a for network for the purpose of monitoring or collecting data about network activity. |
| Rx Power Save Poll | Displays the power save using the PSP *(Power Save Poll )* mode. Power Save Poll is a protocol, which helps to reduce the amount of time a radio needs to powered. PSP allows the WiFi adapter to notify the access point when the radio is powered down. The access point holds any network packet to be sent to this radio. |

The RF Quality Index area displays the following information:

| | |
|---|---|
| RF Quality Index | Displays information on the RF quality of the selected wireless client. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions as well as the retry rate and the error rate. The RF quality index value can be interpreted as:<br>• *0 – 20* (Very low utilization)<br>• *20 – 40* (Low utilization)<br>• *40 – 60* (Moderate utilization)<br>• *60 and above* (High utilization) |
| Retry Rate | Displays the average number of retries per packet. A high number indicates possible network or hardware problems. |
| SNR (dBm) | Displays the connected client's SNR. A high SNR could warrant a different access point connection to improve performance. |
| Signal (dBm) | Displays the power of the radio signals in - dBm. |
| Noise (dBm) | Displays the disturbing influences on the signal in - dBm. |
| Error Rate (ppm) | Displays the number of received bit rates altered due to noise, interference and distortion. It is a unit-less performance measure. |
| MOS Score | Displays average voice call quality using the MOS *(Mean Opinion Score )* call quality scale. The MOS scale rates call quality on a scale of 1-5, with higher scores being better. If the MOS score is lower than 3.5, it's likely users will not be satisfied with the voice quality of their call. |
| R-Value | *R-value* is a number or score used to quantitatively express the quality of speech in communications systems. This is used in digital networks that carry VoIP *(Voice over IP )* traffic. The R-value can range from *1 (worst)* to *100 (best)* and is based on the percentage of users who are satisfied with the quality of a test voice signal after it has passed through a network from a source (transmitter) to a destination (receiver). The R-value scoring method accurately portrays the effects of packet loss and delays in digital networks carrying voice signals. |

4 Select **Refresh** to update the screen's statistics counters to their latest values.

## Client WMM TSPEC

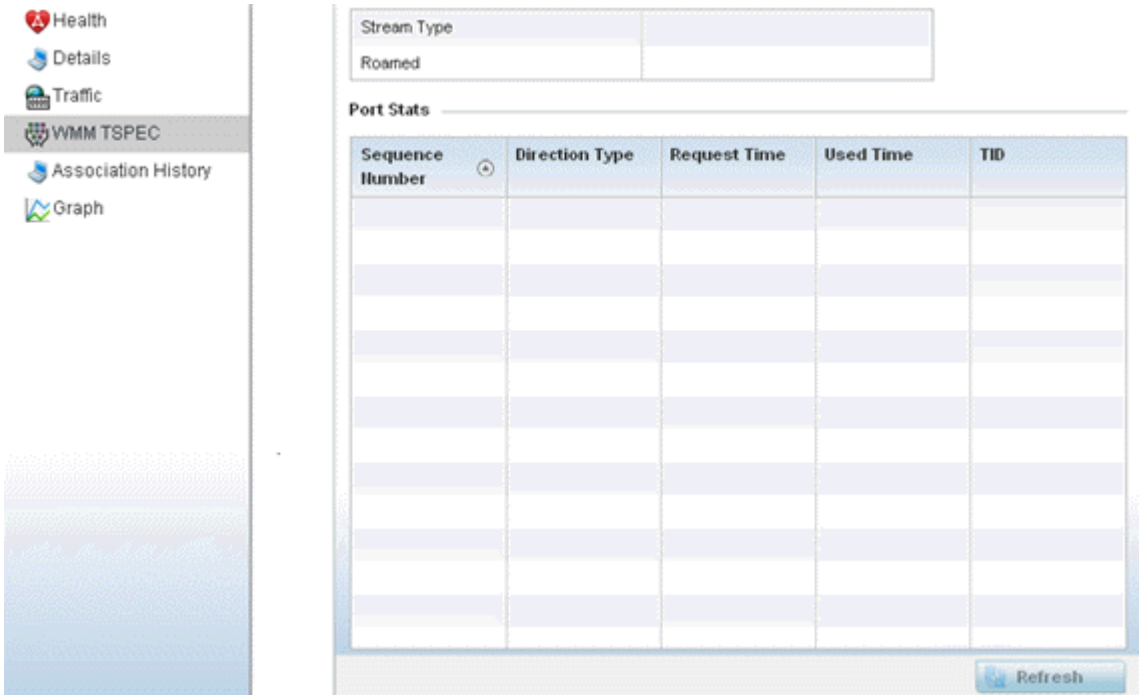
The 802.11e TSPEC *(Traffic Specification)* provides a set of parameters that define the characteristics of the traffic stream, (operating requirement and scheduling etc.). The sender's TSPEC specifies parameters available within packet flows. Both sender and the receiver use TSPEC.

The TSPEC screen provides the information about TSPEC counts and TSPEC types utilized by the selected wireless client.

To view the TSPEC statistics:

1 Select the **Statistics** menu from the Web UI.
2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller, an access point, then a connected client.
3 Select **WMM TPSEC**.

The **Statistics > Wireless Client > WMM TPSEC** screen is displayed.




The top portion of the screen displays the TSPEC stream type and whether the client has roamed.

The Ports Stats field displays the following:

| | |
|---|---|
| Sequence Number | Lists the system assigned sequence number that's unique to this WMM TPSEC **uplink** or **downlink** data stream. |
| Direction Type | Displays whether the WMM TPSEC data stream is in the **uplink** or **downlink** direction. |
| Request Time | Lists each sequence number's request time for WMM TPSEC traffic in the specified direction. This is time allotted for a request before packets are actually sent. |

| | |
|---|---|
| Used Time | Displays the time the client used TSPEC. The client sends a DELTS *(delete traffic stream)* message when it has finished communicating. |
| TID | Displays the parameter for defining the traffic stream. TID identifies data packets as belonging to a unique traffic stream. |

4 Periodically, select **Refresh** to update the screen to its latest values.

## Client Association History

Refer to the **Association History** screen to review this client's access point connections. Hardware device identification, operating channel and GHz band data is listed for each access point. The Association History can help determine whether the client has connected to its target access point and maintained its connection, or has roamed and been supported by unplanned access points in the controller managed network.

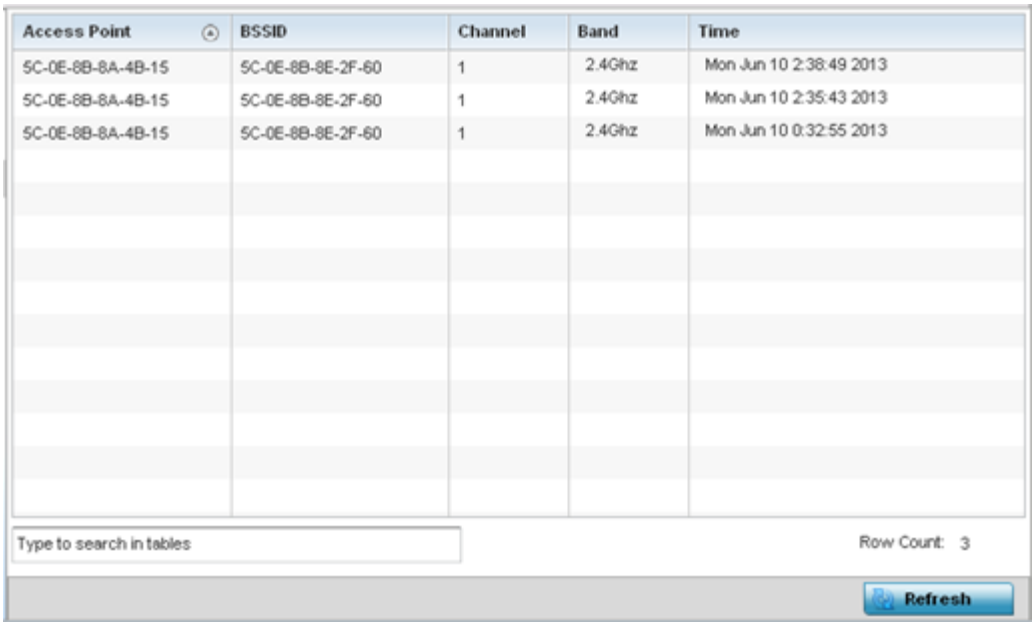
To view a selected client's association history:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller, an access point, then a connected client.

3 Select **Association History**.

The **Statistics > Wireless Client > Association History** screen is displayed.




4 Refer to the following to determine this client's access point association history:

| | |
|---|---|
| access point | Lists the access point MAC address this client has connected to, and is being managed by |
| BSSID | Displays the BSSID of each previously connected access point. |
| Channel | Lists the channel shared by both the access point and client for interoperation, and to avoid congestion with adjacent channel traffic. |

| | |
|---|---|
| Band | Lists the 2.4 or 5GHz radio band this clients and its connect access point are using for transmit and receive operations. |
| Time | Lists the historical connection time between each listed access point and this client. |

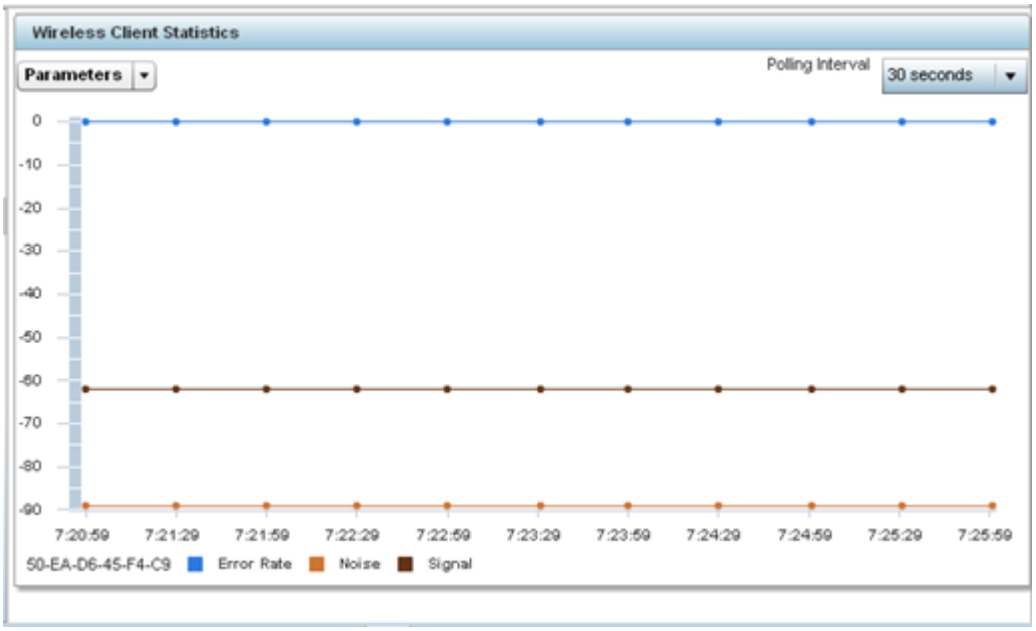
5 Select **Refresh** to update the screen to it's latest values.

## Client Graph

Use the **Graph** to assess a connected client's radio performance and diagnose performance issues that may be negatively impacting performance. Up to three selected performance variables can be charted at one time. The graph uses a Y-axis and a X-axis to associate selected parameters with their performance measure.

To view a graph of this client's statistics:

1 Select the **Statistics** menu from the Web UI.
2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller, an access point, then a connected client.
3 Select **Graph**.
4 Use the **Parameters** drop-down menu to define from 1- 3 variables assessing signal noise, transmit or receive values.
5 Use the **Polling Interval** drop-down menu to define the interval the chart is updated. Options include **`30 seconds`**, **`1 minute`**, **`5 minutes`**, **`20 minutes`** or **`1 hour`**. The default value is *30 seconds*.




6 Select an available point in the graph to list the selected performance parameter, and display that parameter's value and a time stamp of when it occurred.

# 15 WiNG Events

WiNG outputs an event message for configuration changes and status updates to enable an administrator to assess the success or failure of specific configuration activities. Use the information in this chapter to review system generated event messages and their descriptions.

Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication/encryption, and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices. By default, there is no enabled event policy and one needs to be created and implemented.

For more information on the UI's descriptions of events, refer to Fault Management on page 864.

# 16 WiNG Event Messages

| Event | Description |
|---|---|
| ADOPT-SERVICE SNMP_SUCCESS 6 | SNMP framework success |
| ADOPT-SERVICE SNMP_FAILURE 6 | SNMP framework failure |
| ADOPT-SERVICETUT_TEMPERATURE_ALARM_RAISED ([str]) | Temperature alarm raised on sensor |
| ADOPT-SERVICE TUT_TEMPERATURE_ALARM_CLEARED ([str]) | Temperature alarm cleared on sensor |
| ADOPT-SERVICE TUT_TEMPERATURE_ALARM_CLEARED ([str]) | Temperature alarm cleared on sensor |
| ADOPT-SERVICE TUT_FAN_ALARM_CLEARED 5 IPX ([str]) | Fan alarm cleared on ID |
| ADOPT-SERVICE TUT_PWRCTRL_ALARM_RAISED 5 IPX ([str]) | Power controller alarm raised |
| ADOPT-SERVICE TUT_PWRCTRL_ALARM_CLEARED 5 IPX ([str]) | Power controller alarm cleared |
| ADOPT-SERVICE TUT_LINE_POWER_ALARM_RAISED 5 IPX ([str]) Line power alarm raised on id [str] | Line power alarm raised |
| ADOPT-SERVICE TUT_LINE_POWER_ALARM_CLEARED 5 IPX ([str]) Line power alarm cleared on id [str] | Line power alarm cleared |
| ADOPT-SERVICE TUT_WLAN_CLIENT_ASSOC 6 IPX ([str]) Client [str] on interface index [str] associated | Client associated |
| ADOPT-SERVICE TUT_WLAN_CLIENT_DISASSOC 6 IPX ([str]) Client [str] on interface index [str] disassociated with status code [str], [str] | Client disassociated |
| ADOPT-SERVICE TUT_WLAN_CLIENT_ASSOC_FAILURE 3 IPX ([str]) Association failed for Client [str] on interface index [str] with status code [str], [str] | Association failed for client on specified interface index |
| ADOPT-SERVICE TUT_WLAN_CLIENT_AUTH 6 IPX ([str]) | Client on interface index authenticated |
| ADOPT-SERVICE TUT_WLAN_CLIENT_DEAUTH 6 IPX ([str]) | Client on interface index deauthenticated with status code |
| ADOPT-SERVICE TUT_WLAN_CLIENT_AUTH_FAILURE 3 IPX ([str]) | Authentication failed for client on interface index with status code |
| ADOPT-SERVICE TUT_RADIO_ADAPTIVE_POWER_CHANGE 5 IPX ([str]) | Interface with operational status and power levels |
| ADOPT-SERVICE TUT_RF_MONITOR_MODE_CHANGE 5 IPX ([str]) | RF monitor status changed to on interface |

| Event | Description |
|---|---|
| ADOPT-SERVICE IPX_EVENT_FAILURE 3 IPX ([str]) | Failed to raise WiNG event |
| AP NO_IMAGE_FILE [str] firmware image is not present on controller | Access Point firmware not on controller |
| AP IMAGE_PARSE_FAILURE Format of [str] firmware image on controller is invalid | Invalid Access Point firmware file |
| AP LEGACY_AUTO_UPDATE Legacy Access Point [str] [mac] being updated | Legacy Access Point updated |
| AP AP_ADOPTED [str] [mac] adopted | Access Point adopted |
| AP AP_UNADOPTED [str] [mac] un-adopted | Access Point unadopted |
| AP AP_RESET_DETECTED 6 [str] [mac] reset itself | Access Point reset detected |
| AP AP_RESET_REQUEST 6 [str] [mac] reset request | Access Point user requested reset |
| AP AP_TIMEOUT 6 str] [mac] timed out, reset sent to AP | Access Point timed out |
| AP ADOPTED Access Point([qstr]/[qstr]/[dev]) at rf-domain:[qstr] adopted and configured. Radios: Count=[str], Bss: [str] | Access Point adopted and configured |
| AP UNADOPTED Access Point([qstr]/[qstr]/[dev]) at rf-domain:[qstr] unadopted. Radios: Count=[str], Bss: [str] | Access Point unadopted |
| AP ADOPTED_TO_CONTROLLER Joined successfully with controller [qstr]([str]) | Access Point adopted to controller |
| AP ONLINE Access Point [dev] is now online. Offline Reason is [str]. Offline count is [int] | Access Point online |
| AP OFFLINE Access Point [dev] is now offline. Offline Reason is [str]. Offline count is [int] | Access Point offline |
| AP OFFLINE Device [dev]([str]) is offline, last seen:[int] minutes ago on switchport [str] | Adopted device offline |
| AP RESET Reset Access Point mac [dev], [str] | Access Point reset |
| AP ADOPTION_REDIRECTED Access Point([qstr]/[qstr]/[dev]) cdp:[qstr] lldp:[qstr] redirected to the controller host/pair [qstr] - [qstr] | Access Point redirected |
| AP AP_AUTOUP_TIMEOUT 4 AUTOUPGRADE: [str] mac [str] Autoupgrade timed out | Time out while auto upgrading an AP |
| AP AP_AUTOUP_REBOOT 5 AUTOUPGRADE: [str] mac [str] Autoupgrade rebooting | Rebooting AP after upgrade |
| AP AP_AUTOUP_NO_NEED 6 AUTOUPGRADE: [str] mac [str] ver [str] Autoupgrade not required or not available | Auto upgrade not initiated |
| AP AP_AUTOUP_NEEDED 6 AUTOUPGRADE: [str] mac [str] ver [str] Autoupgrade will be applied | Auto upgrade is initiated on AP |
| AP AP_AUTOUP_DONE 5 AUTOUPGRADE: [str] mac [str] Autoupgrade complete | Auto upgrade successful |

| Event | Description |
|---|---|
| AP AP_AUTOUP_FAIL 4 AUTOUPGRADE: [str] mac [str] Autoupgrade failed | Failed auto upgrade attempt |
| AP AP_AUTOUP_VER 6 AUTOUPGRADE: version [str] available for [str] equipment | Available Access Point firmware versions for auto upgrade |
| AAA RADIUS_DISCON_MSG Received Radius dynamic authorization Disconnect Message for [qstr] from server [qstr] | Received RADIUS disconnect request |
| AAA RADIUS_VLAN_UPDATE6 Assigning Radius server specified vlan [uint] to client [qstr] on wlan [qstr] | Client VLAN updated by RADIUS |
| AAA RADIUS_SESSION_NOT_STARTED5 Radius server indicates session time has not started for client [qstr] | Start time from RADIUS resource not yet valid |
| AAA RADIUS_SESSION_EXPIRED5 Radius server indicates session has already expired for client [qstr] | Session time from RADIUS resource already expired |
| ADV-WIPS ADV-WIPS-EVENT-1 4 Detected DoS Deauthentication attack against [mac] [str] | DoS Deauthentication attack |
| ADV-WIPS ADV-WIPS-EVENT-2 4 Detected DoS Disassociation attack against [mac] [str] | DoS disassociation attack |
| ADV-WIPS ADV-WIPS-EVENT-3 4 Detected DoS EAP failure spoof attack by [mac] [str] | EAP failure spoof attack |
| ADV-WIPS ADV-WIPS-EVENT-10 4 Detected ID-Theft out of sequence attack for [mac] [str] | ID theft out of sequence attack |
| ADV-WIPS ADV-WIPS-EVENT-11 4 Detected possible ID-Theft EAPoL Success spoof attack by [mac] [str] | Possible ID theft EAPoL success spoof attack |
| ADV-WIPS ADV-WIPS-EVENT-12 4 Detected possible WLAN-Jack attack by [mac] [str] | Possible WLAN jack attack |
| ADV-WIPS ADV-WIPS-EVENT-13 4 Detected possible ESSID-Jack attack against [mac] [str] | Possible ESSID jack attack |
| ADV-WIPS ADV-WIPS-EVENT-14 4 Detected possible Monkey-Jack attack by [mac] [str] | Possible monkey jack attack |
| ADV-WIPS ADV-WIPS-EVENT-16 4 Detected possible NULL Probe Response attack by [mac] [str] | Possible NULL probe response attack |
| ADV-WIPS ADV-WIPS-EVENT-105 4 Sanctioned MU [mac] detected associated with unsanctioned/ neighboring AP [str] | Sanctioned MU detected associated with unsanctioned/ neighboring AP |
| ADV-WIPS ADV-WIPS-EVENT-109 4 Multicast all systems traffic found from [mac] [str] | Multicast all systems traffic |
| ADV-WIPS ADV-WIPS-EVENT-110 4 Multicast all routers traffic found from [mac] [str] | Multicast all routers traffic |
| ADV-WIPS ADV-WIPS-EVENT-111 4 Multicast OSPF all traffic found from [mac] [str] | Multicast OSPF all traffic |
| ADV-WIPS ADV-WIPS-EVENT-112 4 Multicast OSPF Deisgnated Routers traffic found from [mac] [str] | Multicast OSPF designated routers traffic |
| ADV-WIPS ADV-WIPS-EVENT-113 4 Multicast RIP-2 Routers traffic found from [mac] [str] | Multicast RIP 2 routers traffic |

| Event | Description |
|---|---|
| ADV-WIPS ADV-WIPS-EVENT-114 4 Multicast IGRP Routers traffic found from [mac] [str] | Multicast IGRP routers traffic |
| ADV-WIPS ADV-WIPS-EVENT-115 4 Multicast DHCP Server Relay Agent traffic found from [mac] [str] | Multicast DHCP server relay agent traffic |
| ADV-WIPS ADV-WIPS-EVENT-116 4 Multicast VRRP Agent traffic found from [mac] [str] | Multicast VRRP agent traffic |
| ADV-WIPS ADV-WIPS-EVENT-117 4 Multicast HSRP Agent traffic found from [mac] [str] | Multicast HSRP agent traffic |
| ADV-WIPS ADV-WIPS-EVENT-118 4 Multicast IGMP traffic found from [mac] [str] | Multicast IGMP traffic |
| ADV-WIPS ADV-WIPS-EVENT-119 4 Detected NETBIOS traffic from [mac] [str] | Detected NETBIOS traffic |
| ADV-WIPS ADV-WIPS-EVENT-120 4 Detected STP traffic from [mac] [str] | Detected STP traffic |
| ADV-WIPS ADV-WIPS-EVENT-113 4 Multicast RIP-2 Routers traffic found from [mac] [str] | Multicast RIP 2 routers traffic |
| ADV-WIPS ADV-WIPS-EVENT-121 4 Detected IPX traffic from [mac] [str] | Detected IPX traffic |
| ADV-WIPS ADV-WIPS-EVENT-142 4 Detected possible Probe Response attack by [mac] [str] | Possible probe response attack |
| ADV-WIPS ADV-WIPS-EVENT-221 4 Detected Invalid Management Frames from [mac] [str] | Invalid management frames |
| ADV-WIPS ADV-WIPS-EVENT-26 4 Detected DoS RTS flood attack against [mac] [str] | DoS RTS flood attack |
| ADV-WIPS ADV-WIPS-EVENT-222 4 Detected Invalid Channel Advertisement for [mac] [str] | Invalid channel advertisement |
| ADV-WIPS ADV-WIPS-EVENT-63 4 Detected Windows ZERO Configuration Memory Leak on [mac] [str] | Windows ZERO configuration memory leak |
| ADV-WIPS ADV-WIPS-EVENT-220 4 Detected Unauthorized Bridge [mac] [str] | Unauthorized bridge |
| AP SW_CONN_LOST 0 Lost connectivity with controller after config update. Rebooting and reverting to older working configuration | Controller connectivity lost |
| AAA RADIUS_DISCON_MSG5 Received Radius dynamic authorization Disconnect Message for [qstr] from server [qstr] | Received RADIUS disconnect request |
| AAA RADIUS_VLAN_UPDATE6 Assigning Radius server specified vlan [uint] to client [qstr] on wlan [qstr] | Client VLAN updated by RADIUS resource |
| AAA RADIUS_SESSION_NOT_STARTED5 Radius server indicates session time has not started for client [qstr] | Start time from RADIUS resource not yet valid |
| AAA RADIUS_SESSION_EXPIRED5 Radius server indicates session has already expired for client [qstr] | Session time from RADIUS resource already expired |

| Event | Description |
|---|---|
| CAPTIVE-PORTAL AUTH_SUCCESS6 Captive-portal authentication success for client [mu] ([qstr-ip]) user [qstr] | Authentication sucess |
| ADV-WIPS ADV-WIPS-EVENT-26 4 Detected DoS RTS flood attack against [mac] [str] | DoS RTS flood attack |
| ADV-WIPS ADV-WIPS-EVENT-222 4 Detected Invalid Channel Advertisement for [mac] [str] | Invalid channel advertisement |
| ADV-WIPS ADV-WIPS-EVENT-63 4 Detected Windows ZERO Configuration Memory Leak on [mac] [str] | Windows ZERO configuration memory leak |
| ADV-WIPS ADV-WIPS-EVENT-220 4 Detected Unauthorized Bridge [mac] [str] | Unauthorized bridge |
| AP SW_CONN_LOST 0 Lost connectivity with controller after config update. Rebooting and reverting to older working configuration | Controller connectivity lost |
| AAA RADIUS_DISCON_MSG5 Received Radius dynamic authorization Disconnect Message for [qstr] from server [qstr] | Received RADIUS resource disconnect request |
| AAA RADIUS_VLAN_UPDATE6 Assigning Radius server specified vlan [uint] to client [qstr] on wlan [qstr] | Client VLAN updated by RADIUS |
| AAA RADIUS_SESSION_NOT_STARTED5 Radius server indicates session time has not started for client [qstr] | Start time from RADIUS resource not yet valid |
| AAA RADIUS_SESSION_EXPIRED5 Radius server indicates session has already expired for client [qstr] | Session time from RADIUS resource already expired |
| CAPTIVE-PORTAL AUTH_SUCCESS6 Captive-portal authentication success for client [mu] ([qstr-ip]) user [qstr] | Authentication success |
| CAPTIVE-PORTAL AUTH_FAILED6 Captive-portal authentication failed for client [mu] ([qstr-ip]) | Authentication failed |
| CAPTIVE-PORTAL SESSION_TIMEOUT6 Captive-portal session timed out for client [mu] ([qstr-ip]) | Session timed out |
| CAPTIVE-PORTAL CLIENT_DISCONNECT 6 Captive-portal session disconnected for client [mu] ([qstr-ip]) | Client disconnected |
| CAPTIVE-PORTAL PURGE_CLIENT6 Captive-portal: Purge client [mu] by new client [mu] for user [qstr] | Client purged |
| CAPTIVE-PORTAL FLEX_LOG_ACCESS 6 [qstr]: [qstr] allowed access for client [mu] ([qstr-ip]) | Flex log access granted for client |
| CAPTIVE-PORTAL INACTIVITY_TIMEOUT 6 Captive-portal session cleared for client [mu] ([qstr-ip]) after inactivity timeout | Client timed out due to inactivity |
| CAPTIVE-PORTAL ALLOW_ACCESS6 Captive-portal allow access for client [mu] ([qstr-ip]) | Client allowed access |
| CAPTIVE-PORTAL CLIENT_REMOVED6 Captive-portal session removed for client [mu] ([qstr-ip]) on policy change/admin action | Client removed due to admin changes |

| Event | Description |
|---|---|
| CAPTIVE-PORTAL PAGE_CRE_FAILED3 Page creation failed for policy [qstr], file [qstr], Error [qstr] | Page creation failure |
| CAPTIVE-PORTAL DATA_LIMIT_EXCEED6 Data limit exceed, Usage:[int] KBytes, Action:[str], client [mu] ([ip]) | Client data limit exceeded |
| CAPTIVE-PORTAL VLAN_SWITCH6 Client [mu] ([ip]) switching from vlan [int] to vlan [int] | Client VLAN switch |
| CAPTIVE-PORTAL SERVER_MONITOR_STATE_CHANGE6 Captive-portal policy [qstr]: service monitor [str] server status changing from [qstr] to [qstr] | Captive portal server monitor state changed |
| CAPTIVE-PORTAL NO_SERVICE_PAGE_SENT6 Captive-portal sent no service page to client [mu] ([ip]) as [str] server is down | No service page sent to client |
| CERTMGR RSA_KEY_ACTIONS_SUCCESS 6 [str] of RSA key [str] successful | Successful completion of RSA key related actions (import, export etc.) |
| CERTMGR RSA_KEY_ACTIONS_FAILURE 3 [str] of RSA key [str] failed: [str] | Failure of RSA key related actions (import, export etc.) |
| CERTMGR CA_CERT_ACTIONS_SUCCESS 6 [str] of CA certificate for trustpoint [str] successful | Successful completion of CA certificate related actions (import, export etc.) |
| CERTMGR CA_CERT_ACTIONS_FAILURE 3 [str] of CA certificate for trustpoint [str] failed: [str] | Failure of CA certificate actions (import, export etc.) |
| CERTMGR SRV_CERT_ACTIONS_SUCCESS 6 [str] of Server Certificate of trustpoint [str] successful | Successful completion of server certificate actions (import, export etc.) |
| CERTMGR SVR_CERT_ACTIONS_FAILURE 3 [str] of Server Certificate of trustpoint [str] failed: [str] | Failure of server certificate actions (import, export etc.) |
| CERTMGR CSR_EXPORT_SUCCESS 6 Export of Certificate Signing Request for [str] successful | Successful export of certificate signing request |
| CERTMGR CSR_EXPORT_FAILURE 3 Export of Certificate Signing Request for [str] failed: [str] | Failed to export certificate signing request |
| CERTMGR CRL_ACTIONS_SUCCESS 6 [str] of CRL for trustpoint [str] successful | Successful completion of certificate revocation list action |
| CERTMGR CRL_ACTIONS_FAILURE 3 [str] of CRL for trustpoint [str] failed: [str] | Certificate revocation list action failure |
| CERTMGR DELETE_TRUSTPOINT_ACTION 6 Deletion of trustpoint [str] successful | Deletion of trustpoint |
| CERTMGR IMPORT_TRUSTPOINT 6 Import of Trustpoint [str] [str] | Import of trustpoint |
| CERTMGR EXPORT_TRUSTPOINT 6 Export of Trustpoint [str] [str]// | Export of trustpoint |
| CERTMGR CERT_EXPIRY 4 [str] certificate for trustpoint [str] [str] | Certificate expiration |
| CERTMGR CA_KEY_ACTIONS_SUCCESS 6 [str] of CA private key for trustpoint [str] successful | Successful completion of CA private key actions |

| Event | Description |
|---|---|
| CERTMGR CA_KEY_ACTIONS_FAILURE 3 [str] of CA private key for trustpoint [str] failed: [str] | Failure of CA private key actions |
| CLUSTER CMASTER_CFG_UPDATE_FAIL 3 Cluster master config update to [str] failed, Err: [str] | Cluster master config update failed |
| CLUSTER MAX_EXCEEDED 4 Max cluster members ([uint]) exceeded, clustering will not function properly until corrected | Max cluster count exceeded |
| CLUSTER STATE_CHANGE 4 Active cluster member changed. Present active [str]. Previous active [str]. | Active cluster membership change |
| CLUSTER STATE_CHANGE_INACTIVE 4 Member [str] (load[int]) changing state from Active to Standby. New member [str] standby load [int]. | Cluster member change from active to standby |
| CLUSTER STATE_CHANGE_ACTIVE 4 Member [str] (load[int]) changing state from Standby to Active. New member [str] standby load [int] | Cluster member change from standby to active |
| CLUSTER STATE_RETAIN_ACTIVE 4 Member [str] (load[int]) retaining Active state. New member [str] standby load [int] | Cluster member retaining active state |
| CRM CRITICAL_RESOURCE_UP5 Critical Resource [str] is UP | Critical resource is up |
| CRM CRITICAL_RESOURCE_DOWN 5 Critical Resource [str] is DOWN | Critical resource is down |
| CERTMGR-LITE INVALIDCACERT 5 CA Certificate imported for the trustpoint [str] is invalid | CA certificate is invalid |
| CERTMGR-LITE INVALIDSERVCERT 5 Server Certificate imported for the trustpoint [str] is invalid | Server certificate is invalid |
| CERTMGR-LITE INVALIDCERTCRL 5 Certificate Crl Imported for trustpoint [str] is invalid | CRL is invalid |
| CERTMGR-LITE CERTEXPIRED 5 [str] Certificate of trustpoint [str] is expired// | Certificate is expired |
| CERTMGR-LITE INVALIDCERTKEY 5 Private key imported for trustpoint [str] is not valid | Private key is invalid |
| CERTMGR-LITE INVALIDRSAKEY 5 Rsakey imported is not valid [str] is invalid// | RSA key import operation |
| CERTMGR-LITE KEYDECRYPTFAILE 4 Rsakey cannot be decrypted with the password provided | RSA key cannot be decrypted with provided password |
| CERTMGR-LITE CERTIMPORTED 6 [str] Certificate imported for the trustpoint [str] | Certificate imported for trustpoint |
| CERTMGR-LITE CERTKEYIMPORTED 6 Private key imported for the trustpoint [str] | Private key imported for trustpoint |
| CERTMGR-LITE RSAKEYIMPORTED 6 Rsakey imported with the name [str] | RSA key imported |
| CERTMGR-LITE DELETETRUSTPOINT 6 Trustpoint [str] is deleted | Trustpoint deleted |

| Event | Description |
|---|---|
| CERTMGR-LITE DELETERSAKEY 6 Rsakey [str] is deleted | RSA Key deleted |
| CERTMGR-LITE CERTREQUESTGEN 6 Certificate request generated for the trustpoint [str] | Certificate requested generated |
| CERTMGR-LITE CERTSELFSIGNEDGEN 6 Selfsigned certificate generated for the trustpoint [str] | Self signed certificate generated |
| CERTMGR-LITE RSAKEYGEN 6 Rsa key [str] generated | RSA key generated |
| CERTMGR-LITE ERROR 5 [str] | Certificate manager general error |
| CERTMGR-LITE CERT_EXPIRY4 [str] certificate for trustpoint [str] [str] | Certificate about to expire |
| CERTMGR CERT_RENEW_FAILED1 Certificate renew in field failed reason [str] | Certificate renew failure reason |
| DHCPSVR DHCPSVR_STOP 6 DHCP server is stopped | DHCP server stopped |
| DIAG WD_RESET_SYS 2 The system has been RESET by the Watchdog | Log watchdog reset |
| DIAG CPU_USAGE_TOO_HIGH 4 CPU Usage too high. Limit of [int]*(0.1%) exceeded. Current CPU usage is [int]*(0.1%) | Log CPU load detected as too high |
| DIAG CPU_USAGE_TOO_HIGH_RECOVER 4 CPU Usage too high recover. Limit is [int]*(0.1%) | Current CPU usage is too high |
| DIAG CPU_LOAD 4 [str] minute average load limit exceeded, value is [str]% limit is [str]% (top processes: [str]) | CPU average load limit exceeded |
| DIAG RAM_USAGE 6 [str], pid [uint], has exceeded ram usage limit [uint].[uint]%, now using [uint].[uint]% | Log processor RAM usage has exceeded RAM limit |
| DIAG MEM_USAGE_TOO_HIGH 6 Memory Usage too high. Current Usage is [int]*(0.1%). Memory Usage Threshold is [int]*(0.1%) | Memory usage too high |
| DIAG MEM_USAGE_TOO_HIGH_RECOVER 6 Memory Usage too high recover. Current Usage is [int]*(0.1%). Memory Usage Threshold is [int]*(0.1%) | Memory usage detected as too high |
| DIAG BUF_USAGE 6 [uint] byte buffer usage greater than expected, [uint] used, warning level [uint] | Log buffer usage greater than anticipated |
| DIAG HEAD_CACHE_USAGE 6 socket buffer head cache usage is greater than expected, usage [uint], warning level [uint] | Log head cache usage greater than anticipated |
| DIAG IP_DEST_USAGE 6 IP destination cache usage is greater than expected, usage [uint], warning level [uint] | Log destination cache usage greater than anticipated |
| DIAG FREE_RAM 6 Free RAM, [str]% is less than limit [str]%. Top Memory process: [str]/[uint] using [uint].[uint]% , [str]/[uint] using [uint].[uint]% , [str]/[uint] using [uint].[uint]% | Log RAM space less than limit |
| DIAG FREE_FLASH_DISK 4 Free [str] file system space, [str]% is less than limit [str]% | Log free disk space less than limit |

| Event | Description |
|---|---|
| DIAG DISK_USAGE 4 Disk usage too high | Log disk usage too high |
| "DIAG NEW_LED_STATE 6 LED state message [str] from module [str] | Log LED message from module |
| DIAG FREE_FLASH_INODES 4 [uint] Free INodes on [str] file system is less than limit [uint] | Log INodes less than system limit |
| DIAG FREE_NVRAM_DISK 4 Free [str] file system space, [str]% is less than limit [str]% | Log file system space less than limit |
| DIAG FREE_NVRAM_INODES 4 [uint] Free INodes on [str] file system is less than limit [uint] | Log free INodes on file system less than limit |
| DIAG FREE_RAM_DISK 4 Free [str] file system space, [str]% is less than limit [str]% | Log free file system space less than limit |
| DIAG FREE_RAM_INODES 4 [uint] Free INodes on [str] file system is less than limit [uint] | LOG_FREE_VARFS_INODES |
| DIAG FD_COUNT 4 FD Usage [uint] is over limit [uint] | HUMM |
| DIAG DISK_USAGE 4 Disk usage too high | Log disk utilization usage too high |
| DIAG NEW_LED_STATE 6 LED state message [str] from module [str] | Log LED state message from module |
| DIAG LED_IDENTIFY 6 LED identify sequence [str] | Log identification sequence |
| "DHCPSVR RELAY_NO_IFACE 4 Dhcp relay cannot be allowed on interface [str] as it does not exist | No interface for DHCP relay |
| DHCPSVR RELAY_IFACE_NO_IP 4 Dhcp relay cannot be allowed on interface [str] as it does not have an IP address | No IP address on DHCP relay interface |
| DHCPSVR RELAY_START 6 DHCP relay agent started on [str] | DHCP relay agent started |
| DHCPSVR RELAY_STOP 6 DHCP relay agent stopped | DHCP relay agent stopped |
| DHCPSVR DHCPSVR_START 6 DHCP server is started | DHCP server started |
| DIAG FAN_UNDERSPEED 4 Fan [str] under speed: [uint] RPM is under limit [uint] RPM | Fan speed under set RPM limit |
| DIAG ELAPSED_TIME 7 Elapsed time since last diag run appears to be zero | Log elapsed time since last diagnostic run |
| DIAG AUTOGEN_TECH_SPRT 6 Auto generated tech-support dump file [str] [str] | Log generation of tech support dump file |
| DIAG POE_INIT_FAIL 3 Could not initialize the PoE manager | Log PoE manager intialization failure |
| DIAG POE_POWER_LEVEL 4 POE power consumption is [uint]W which exceeds [uint]% of [uint]W power budget | Log power consumption exceeds power budget limit |
| DIAG POE_READ_FAIL 3 Could not read from the PoE | Log PoE read failure |
| DIAG POE_STATE_CHANGE 4 port [uint] POE state changed to [str] | Log PoE state change |
| DIAG RAID_DEGRADED 4 RAID array is degraded | Log RAID array degraded |

| Event | Description |
|---|---|
| DIAG RAID_ERROR 4 RAID array management error [uint] | Log RAID array management error |
| DIAG PWRSPLY_FAIL 4 Power supply failure, no longer redundant | Log power supply failure |
| DIAG HDD_FAILING 4 HDD is failing | Log HDD failure |
| DIAG UNDER_VOLTAGE 4 Voltage [str]V under low limit [str]V | Log voltage sensor under low limit |
| DIAG OVER_VOLTAGE 4 Voltage [str]V over high limit [str]V | Log voltage sensor over high limit |
| DIAG LOW_TEMP 6 Temp sensor [str] [str]C under low limit [str]C | Log temperature sensor under low limit |
| DIAG HIGH_TEMP 4 Temp sensor [str] [str]C over high limit [str]C | Log temperature sensor over high limit |
| DIAG OVER_TEMP 0 Temp sensor [str] [str]C over maximum limit [str]C Shutdown switch | Log temperature sensor over max limit |
| DIAG WD_STATE_CHANGE 6 Watchdog is now [str] | Log watchdog state |
| DOT1X DOT1X_SUCCESS 6 Client [qstr] 802.1x/EAP authentication success on interface [qstr]//802.1x authentication successful | 802.1X authentication successful |
| DOT1X DOT1X_FAILED 5 Client [qstr] failed 802.1x/EAP authentication on interface [qstr]//802.1x authentication failure | 802.1X authentication failed |
| DOT11 COUNTRY_CODE 5 Country of operation configured to [str] | Country of operation configured |
| DOT11 COUNTRY_CODE_ERROR 1 Error setting country of operation. [str] | Error setting country of operation |
| DOT11 CLIENT_ASSOCIATED 6 Client [qstr] associated to wlan [qstr] ssid [qstr] on radio [qstr] | Client associated event |
| DOT11 CLIENT_DISASSOCIATED 6 Client [qstr] disassociated from wlan [qstr] radio [qstr]: [str] (reason code:[uint]) | Client disassociated |
| DOT11 CLIENT_DENIED_ASSOC 5 Client [qstr] denied association on radio [qstr] [str]: [str] | Client denied association |
| DOT11 CLIENT_ASSOC_IGNORED 6 Client [qstr] ignored association on radio [qstr] [str]: [str] | Client ignored association |
| DOT11 WPA_WPA2_SUCCESS 6 Client [qstr] completed [str] handshake on wlan [qstr] radio [qstr] | Client completed WPA/WPA2 handshake |
| DOT11 WPA_WPA2_FAILED 5 Client [qstr] failed [str] handshake on wlan [qstr] radio [qstr] | Client failed WPA/WPA2 handshake |
| DOT11 WPA_WPA2_KEY_ROTN 6 Rotating wpa/wpa2 group keys on wlan [qstr] / | Rotating WPA/WPA2 group keys on WLAN |
| DOT11 TKIP_MIC_FAIL_REPORT 5 TKIP message integrity check failure reported by [mac] on wlan [qstr] | TKIP MIC failure report |

| Event | Description |
|---|---|
| DOT11 TKIP_MIC_FAILURE 5 TKIP message integrity check failed in packet from [mac] on wlan [qstr] | TKIP MIC check failed |
| DOT11 TKIP_CNTRMEAS_START 4 Initiating TKIP countermeasures on wlan [qstr] ssid [qstr] | TKIP countermeasures initiated |
| DOT11 TKIP_CNTRMEAS_END 4 TKIP countermeasures ended on wlan [qstr] ssid [qstr] // | TKIP countermeasures ended |
| DOT11 EAP_SUCCESS 6 Client [qstr] 802.1x/EAP (type: [str]) authentication success on wlan [qstr] radio [qstr] username [str] | EAP authentication success |
| DOT11 EAP_FAILED 5 Client [qstr] failed 802.1x/EAP authentication on wlan [qstr] radio [qstr] | EAP authentication failure |
| DOT11 EAP_CLIENT_TIMEOUT 5 Client [qstr] timeout attempting 802.1x/EAP authentication on wlan [qstr] radio [qstr] | EAP authentication timed out |
| DOT11 EAP_SERVER_TIMEOUT 5 Radius server [str] timeout authenticating client [qstr] on wlan [qstr] radio [qstr] | RADIUS server timed out |
| DOT11 EAP_CACHED_KEYS 6 Key Cache used for client [qstr] on wlan [qstr] radio [qstr]. Skipping 802.1x | Key cache used for authentication |
| DOT11 EAP_OPP_CACHED_KEYS 6 Opportunistic Key Cache used for client [qstr] on wlan [qstr] radio [qstr]. Skipping 802.1x. | Opportunistic key caching used for authentication |
| DOT11 EAP_PREAUTH_SUCCESS 6 Client [qstr] 802.1x/EAP (type:[str]) pre-authentication success on wlan [qstr] bss [mac] | EAP pre authentication success |
| DOT11 EAP_PREAUTH_FAILED 5 Client [qstr] failed 802.1x/EAP pre-authentication on wlan [qstr] bss [mac] | EAP pre-authentication failed |
| DOT11 EAP_PREAUTH_CLIENT_TIMEOUT 5 Client [qstr] timeout attempting 802.1x/EAP pre-authentication on wlan [qstr] | EAP pre-authentication client timeout detected |
| DOT11 EAP_PREAUTH_SERVER_TIMEOUT 5 Radius server [qstr] timeout pre-authenticating client [qstr] on wlan [qstr] | EAP pre-authentication server timeout detected |
| DOT11 FT_ROAM_SUCCESS 6 Client [qstr] fast bss transition roam to wlan [qstr] ssid [qstr] on radio [qstr] | Client fast BSS transition roam to WLAN SSD ID on radio |
| DOT11 GAL_RX_REQUEST 6 Received request to validate [qstr] on global assoc-list [qstr] from [qstr] on rf-domain [qstr] | Received request to validate global association request for RF Domain |
| DOT11 GAL_TX_RESPONSE 6 Sending global assoc-list [qstr] response for [qstr] to [qstr] on rf-domain [qstr], result: [str] | Sending global association response for RF Domain |
| DOT11 GAL_VALIDATE_REQ 6 Sending global assoc-list validation request to controller for [qstr] | Sending global association list validation to controller |
| DOT11 GAL_VALIDATE_FAILED 6 Received global assoc-list validation failure for [qstr] | Received global association list validation failures |

| Event | Description |
|---|---|
| DOT11 GAL_VALIDATE_SUCCESS 6 Received global assoc-list validation success for [qstr] | Received global association list validation successes |
| FWU FWUDONE 6 Firmware update successful, new version is [str] | Update successfully completed |
| FWU FWUABORTED 6 Firmware update aborted | Update aborted |
| FWU FWUNONEED 6 Firmware update not required, running and update versions same [str] | Update not required, running and update version are the same |
| FWU FWUSYSERR 3 Firmware update unsuccessful, system cmd [str] failed | Update unsuccessful, system cmd failed |
| FWU FWUBADCONFIG 3 Firmware update unsuccessful, unable to read configuration file | Update unsuccessful, unable to read config file |
| FWU FWUSERVERUNDEF 3 Firmware update unsuccessful, update server undefined | Update unsuccessful, server undefined |
| FWU FWUFILEUNDEF 3 Firmware update unsuccessful, update file undefined | Update unsuccessful, update file undefined |
| FWU FWUSERVERUNREACHABLE 3 Firmware update unsuccessful, server [str] unreachable | Update unsuccessful, server unreachable |
| FWU FWUCOULDNTGETFILE 3 Firmware update unsuccessful, couldn't get file, [str] // | Update unsuccessful, could not get file |
| FWU FWUVERMISMATCH 3 Firmware update unsuccessful, version mismatch, expected [str], actual [str] // | Update unsuccessful, version mismatch |
| FWU FWUPRODMISMATCH 3 Firmware update unsuccessful, product mismatch, expected [str], actual [str] | Update unsuccessful, product mismatch |
| FWU FWUCORRUPTEDFILE 3 Firmware update unsuccessful, corrupted firmware file | Update unsuccessful, corrupted file |
| FWU FWUSIGNMISMATCH 3 Firmware update unsuccessful, signature mismatch, [str] | Update unsuccessful, signature mismatch |
| FWU FWUUNSUPPORTEDHW 3 Firmware update unsuccessful, unsupported hardware | Update unsuccessful, unsupported hardware version |
| FWU FWUUNSUPPORTEDMODELNUM 3 Firmware update unsuccessful, unsupported FIPS model number | Update unsuccessful, unsupported FIPS model number |
| ISDN_EMERG 0 Emergency: [str] | ISDN emergency |
| ISDN_ALERT 1 Alert: [str] | ISDN alert |
| ISDN_CRIT 2 Critical: [str] | ISDN critical |
| ISDN_ERR 3 Error: [str] | ISDN error |
| ISDN_WARNING 4 Warning: [str] | ISDN warning |
| ISDN_NOTICE 5 Notice: [str] | ISDN notice |
| ISDN_INFO 6 Info: [str] | ISDN information |
| ISDN_DEBUG 7 Debug: [str] | ISDN debug |

| Event | Description |
|---|---|
| L2TPV3 L2TPV3_TUNNEL_UP 5 L2TPV3 tunnel [str] is UP | L2TPV3 tunnel is up |
| L2TPV3 L2TPV3_TUNNEL_DOWN 5 L2TPV3 tunnel [str] is DOWN | L2TPV3 tunnel is down |
| LICMGR LIC_INSTALLED 6 [str] license installed | License installation |
| LICMGR LIC_INSTALL_DEFAULT 6 [str] default license installed, count: [int] | Default license installation |
| LICMGR LIC_INSTALL_COUNT 6 [str] license installed, count: [int] | License count |
| LICMGR LIC_REMOVED 6 [str] license removed | License removed |
| LICMGR LIC_INVALID 3 [str] license invalid Error: [str] | License installation failed |
| MESH MESH_LINK_UP 5 Mesh link up between radio [qstr] and radio [qstr] | Mesh link up |
| MESH MESH_LINK_DOWN 5 Mesh link down between radio [qstr] and radio [qstr] | Mesh link down |
| MGMT LOG_KEY_DELETED 4 Rsakey [str] associated with ssh is deleted so ssh is restarted with default rsa key | RSA key associated with SSH is deleted |
| MGMT LOG_KEY_RESTORED 6Rsakey [str] associated with ssh is added so ssh is restarted with new key | RSA key associated with SSH is added |
| MGMT LOG_TRUSTPOINT_DELETED 4 Trustpoint [str] associated with https is deleted or expired so https is restarted with default trustpoint | Trustpoint associated with HTTPS is deleted |
| MGMT LOG_HTTP_START 5 [str] started in external mode | Web server started in external mode |
| MGMT LOG_HTTP_LOCAL_START 5 thttpd started in localhost mode | Web server started in local mode |
| MGMT LOG_HTTPS_START 5 stunnel started | Secure Web server started |
| MGMT LOG_HTTPS_WAIT 5 waiting for thttpd to start | Waiting for Web server to start |
| MGMT LOG_HTTP_INIT 5 [str] status started is [uint] and external mode is [uint] | Web server started |
| MESH MESHPOINT_LOOP_PREVENT_ON 4 Meshpoint [qstr] loop prevention on (port [str]), wired traffic is blocked | Wired traffic is blocked |
| MESH MESHPOINT_LOOP_PREVENT_OFF 4 Meshpoint loop prevention off (port [str]), all wired traffic is allowed | Wired traffic is allowed |
| MESH MESHPOINT_ROOT_CHANGE 6 Meshpoint [qstr] root changed from [mac] to [mac] via next hop [mac] | Meshpoint root changed |
| MESH MESHPOINT_PATH_CHANGE 6 Meshpoint [qstr] next hop changed from [mac] to [mac] for [mac] | Meshpoint next hop changed |
| NSM IFUP 4 Interface [str] is up | Interface up |
| NSM IFDOWN 4 Interface [str] is down | Interface down |

| Event | Description |
|---|---|
| NSM DHCPIP 6 Interface [str] acquired IP address [ip]/[uint] via DHC | Interface assigned DHCP IP address |
| NSM DHCPDEFRT 6 Default route with gateway [ip] learnt via DHC | Default route learnt via DHCP |
| NSM DHCPIPCHG 5 Interface [str] changed DHCP IP - old IP: [ip]/[uint], new IP: [ip]/[uint] | DHCP Interface IP changed |
| NSM DHCPNODEFRT 5 Interface [str] lost its DHCP default route | Interface no default route |
| NSM IFIPCFG 3 Interface [str] IP address [str] Interface [str] | Interface IP address |
| NSM DHCPC_ERR 3 Both, DHCP client and server are configured for interface [str]. DHCP Client has been enabled on the interface and dhcp server is shut down | DHCP server-client config conflict |
| NSM DHCPIPNOADD 5 Interface [str] lost its DHCP IP address to interface [str]'s overlapping static configured IP address | DHCP IP overlaps static IP address |
| NSM DHCPLSEXP 5 Interface [str] lost its DHCP IP address [ip] due to lease expiration | Interace DHCP lease expired |
| NSM DHCPNAK 5 Interface [str] lost its DHCP IP address [ip], DHCP NAK response from server | DHCP Server returned DHCP NAK response |
| NSM NSM_NTP 6 Look up host [str] [str]// | Translate host name |
| NSM IF_FAILOVER 5 Interface [str] failover to Interface [str] | Interface failover |
| NSM IF_FAILBACK 5 Interface [str] failback to Interface [str] | Interface failback |
| PM PROCSTART 6 Starting process [str] | Process started |
| PM PROCRSTRT 3 Process str]"is not responding. Restarting process | Process restarted |
| PM PROCMAXRSTRT 1 Process [str] reached its maximum number of allowed restarts | Process reached max number of restarts |
| PM PROCSYSRSTRT 0 Process [str] reached its maximum number of allowed restarts. Rebooting the system. | Process reached max restarts. Rebooting system. |
| PM PROCSTOP 5 Process [str] has been stopped | Process has been stopped |
| PM PROCID 5 Process [str] changed its PID from [int] to [int] | Process changed PID |
| PM STARTUPCOMPLETE 5 System startup complete | System startup completed |
| PM PROCNORESP 4 Process [str] is not responding ([uint]/[uint]) | Process is not responding |
| RADCONF RADIUSDSTART 6 Radius Server Started | RADIUS server started |
| RADCONF RADIUSDSTOP 6 Radius Server Stopped | RADIUS server stopped |
| RADCONF COULD_NOT_STOP_RADIUSD 3 radiusd could not be stopped | RADIUS server failed to stop |

| Event | Description |
|---|---|
| RADIO RADIO_STATE_CHANGE 5 Radio [qstr] changing state from [qstr] to [qstr] | Radio state changed |
| RADIO RADAR_SCAN_STARTED 6 Radar scan on primary channel [uint] freq [uint] MHz for a duration [uint] secs on radio [qstr] | Radar scan started |
| RADIO RADAR_SCAN_COMPLETED 6 Radar scan done on primary channel [uint] freq [uint] MHz on radio [qstr] | Radar scan completed |
| RADIO RADAR_DETECTED 4 Radar found on channel [uint] freq [uint] MHz | Radar detected |
| RADIO RADAR_DET_INFO 4 Radar info: Radio: [qstr]. New channel: [uint] freq [uint] MHz. Scan time: [uint] secs | Radar info |
| RADIO RESUME_HOME_CHANNEL 6 Operation on home channel [uint] freq [uint] MHz resumes on radio [qstr] after earlier radar detect | Radio resuming on home channel |
| RADIO ACS_SCAN_STARTED 6 ACS scan started on radio [qstr] | ACS scan started |
| RADIO ACS_SCAN_COMPLETE 6 ACS scan done, channel [uint] selected on radio [qstr] | ACS scan complete |
| RADIO_ANTENNA_ERROR 3 antenna type [str] in is not supported on radio [uint] of device [str] | Invalid (unsupported) antenna detected on this radio |
| RADIO CHANNEL_COUNTRY_MISMATCH 3 Channel [str] not valid in country of operation [str] for [str] [str] | Channel and country of operation mismatch |
| SYSTEM HTTP_ERR 3 [str] did not start | Web server did not start |
| SYSTEM LOGIN_FAIL_BAD_ROLE 3 Log-in failed - [qstr] is an undefined user role - user [qstr] from [qstr] | Failed login attempt - no such user role |
| SYSTEM LOGOUT 6 Logged out user [qstr] with privilege [qstr] from [qstr] | Logout event |
| SYSTEM WARM_START 6 System Warm Start Reason : [str] Timestamp: [str] | System warm start |
| SYSTEM WARM_START_RECOVER 6 Warm Start Recover. Reason: [str] Timestamp: [str] | System wam start recovery |
| SYSTEM COLD_START 6 System Cold start. System came up at [str] | System cold start |
| SYSTEM SERVER_UNREACHABLE 5 Server not reachable, trying authentication using local database . | Authentication using the local database |
| SYSTEM PERIODIC_HEART_BEAT 3 Periodic Heart Beat. Interval:[int]. Ip address [str]. | Periodic heartbeat detected |
| SYSTEM CONFIG_COMMIT 6 Configuration commit by user [qstr] ([str]) from [qstr] | Configuration commit |
| SYSTEM CONFIG_REVISION 6 Configuration revision updated to [str] from [str] | Configuration updated |

| Event | Description |
|---|---|
| SYSTEM SYSTEM_AUTOUP_ENABLE 6 Autoupgrade enabled for [str] | Auto upgrade module is enabled |
| SYSTEM SYSTEM_AUTOUP_DISABLE 6 Autoupgrade disabled for [str] | Auto upgrade module is disabled |
| SYSTEM MAAT_LIGHT 5 MAAT Light module [str] | Notice on action on RIM radio(s) from Maat Light module |
| SYSTEM DEVUP_RFD_FAIL 4 Upgrade failed on mac [str] in RF domain [str] | Upgrade for device failed on rf-domain manager |
| SMTPNOT SMTPAUTH 5 Authentication failure for user: [str] on server [str].// | User authentication failure |
| SMTPNOT NET 5 Network error contacting server: [str]. | Cannot contact server |
| SMTPNOT SMTPINFO 6 [str]. | SMTP information notice |
| SMTPNOT CFG 5 Error reading configuration file. | Cannot read configuration |
| SMTPNOT CFGINC 5 Incomplete Configuration. | Incomplete configuration |
| SMTPNOT SMTPERR 5 [str]. | SMTP 5XX errors |
| SMTPNOT PROTO 5 Protocol Error: [str]. | SMTP protocol errors |
| SYSTEM PROC_STOP 6 Stopping process [qstr] | Stopping process |
| SYSTEM CLOCK_RESET 6 System clock reset, Time: [str] | System clock reset |
| SYSTEM LOGIN 5 Successfully logged in user [qstr] with privilege [qstr] from [qstr] | Successful login |
| SYSTEM LOGIN_FAIL 3 Log-in failed for user [qstr] from [qstr] | Failed login attempt - user authentication failed |
| SYSTEM LOGIN_FAIL_ACCESS 3 Log-in failed - user [qstr] is not allowed access from [qstr] | Failed login attempt - access violation |
| VRRP VRRP_STATE_CHANGE 5 [str]: VRRP Group [uint] transitioned to [str] state | VRRP state transition |
| VRRP VRRP_VIP_SUBNET_MISMATCH 2 VRRP Group [uint] VIP [ip] does not overlap with any of the interface addresses | VRRP IP not overlapping with interface addresses |
| VRRP VRRP_MONITOR_CHANGE 5 [str]: VRRP Group [uint] monitored [str] state change to [str]; priority change from [uint] to [uint] | VRRP monitor link state change |
| WIPS UNSANCTIONED_AP_ACTIVE 6 Unsanctioned AP [mac] vendor [str] on channel [int] with rssi [int] active from [str] | Unsanctioned AP active |
| WIPS UNSANCTIONED_AP_INACTIVE 6 Unsanctioned AP [mac] vendor [str] inactive from [str] | Unsanctioned AP inactive |
| WIPS UNSANCTIONED_AP_STATUS_CHANGE 6 Unsanctioned AP [mac] vendor [str] status has been administratively changed | Unsanctioned AP changed state |

| Event | Description |
|---|---|
| WIPS ROGUE_AP_ACTIVE 4 Rogue AP [mac] vendor [str] on channel [int] with vlan [int] and rssi [int] active from [str] // | Rogue AP active |
| WIPS ROGUE_AP_INACTIVE 4 Rogue AP [mac] vendor [str] inactive from [str] | Rogue AP inactive |
| WIPS AIR_TERMINATION_INITIATED 4 Air termination of [mac] vendor [str] on channel [int] initiated | Air termination initiated |
| WIPS AIR_TERMINATION_ENDED 4 Air termination of [mac] vendor [str] ended | Air termination ended |
| | |
| | |
| | |
| | |
| | |
| | |

# A AP505 and AP510: Dual Mode Capability



## Understanding Dual Mode Capability

The WiNG 7.1 AP505 and AP510 model access points have the capability of operating in the following two modes: **Distributed** and **Centralized**. For a newly-manufactured, out-of-the-box AP505 and AP510 access point the mode of operation is *not specified*. The *Centralized* mode of operation is ideally suited for dense localized deployments, while the *Distributed* mode supports scaled-out deployments.

Refer to the following sections for more information:


- Auto-discovery of AP's Mode of Operation on page 1123
- Manually-setting AP's Mode of Operation on page 1124


### Auto-discovery of AP's Mode of Operation

When a newly-manufactured AP5XX access point boots up for the first time it goes through the following procedure:

1. The AP runs the discovery image to determine its mode of operation.
2. If the AP finds Distributed discovery methods, it reboots into the '*Distributed*' mode.
3. If the AP finds Centralized discovery methods, it reboots into the '*Centralized*' mode.
4. The AP then tries to discover and adopt to an adopter. The following adoption scenarios are possible for the two modes of operation:
   - AP in Distributed mode — can adopt to a WiNG VC, WiNG Controller or ExtremeCloud Appliance
   - AP in Centralized mode — can adopt to ExtremeCLoud Appliance

Note
If the AP (Centralized or Distributed) adopts to ExtremeCloud Appliance, its final mode of operation is determined by the type of site in which the AP is placed. If it is placed in a Distributed site, its mode is set to 'Distributed'. If placed in a 'Centralized site', its mode is set to 'Centralized'. For more information on ExtremeCloud Appliance adoption and configuration, please refer to the ExtremeCloud Appliance User Guide available at https://extremenetworks.com/documentation.

Note
If the AP fails to adopt to any of the above mentioned adopters, you can manually set the AP to the **Standalone** mode. For more information, see Manually-setting AP's Mode of Operation on page 1124.

Note
For information on how to reset the mode of operation of an AP adopted to a WiNG VC or Controller, see Resetting an AP's Mode of Operation on page 1126.

## Manually-setting AP's Mode of Operation

You will need to manually set the AP's mode of operation if:

- the AP boots up for the first time and is unable to discover and adopt to any of the following adopter options: **`WiNG (VC)`**, **`WiNG Controller`**, **`ExtremeCloud Appliance`**.
- you want to deploy the AP as a **`Standalone/WiNG`** or as **`WiNG Virtual Controller`**.

You can either use the AP's CLI or GUI to set the mode of operation.

### *Using CLI to Set AP's Mode of Operation*

To manually set the AP's mode of operation using its CLI:

1 Access the AP's CLI through SSH or console using default credentials.

Use the AP's Primary or Secondary (ZEROCONF) IP address to do an SSH.

Primary IP address - This is the DHCP provided IP address.

Secondary IP address - This is the ZEROCONF IP address '169.254. xx.yy'. Where, '`xx`' and '`yy`' are the last two octets of the AP's MAC address in decimal format. Note, the AP's MAC address will be printed on the box.

For example:

If AP's MAC address is: *00:C0:23:00:**F0:0A***

The secondary IP address will be: *169.254.**240.10***

You will be presented with the following message:

```
AP adoption discovery process in progress…
To cancel and boot in Standalone mode, type (s):
```

2 Type '`s`' to move into the '`Standalone/WiNG`' mode.

```
AP adoption discovery process in progress…
To cancel and boot in Standalone mode, type (s): s

AP booting in Standalone mode…
```

The AP will reboot immediately. After reboot, you will be presented with the WiNG login prompt.

3 Use the following default credentials to login:

username: `admin`

password: `admin123`

### *Using GUI to Set AP's Mode of Operation*

To manually set the AP's mode of operation using its GUI:

1 Access the AP's GUI through a Web browser (http://<AP-IP-ADDRESS>).

Point the Web browser to the AP's Primary or Secondary (ZEROCONF) IP address.

Primary IP address - This is the DHCP provided IP address.

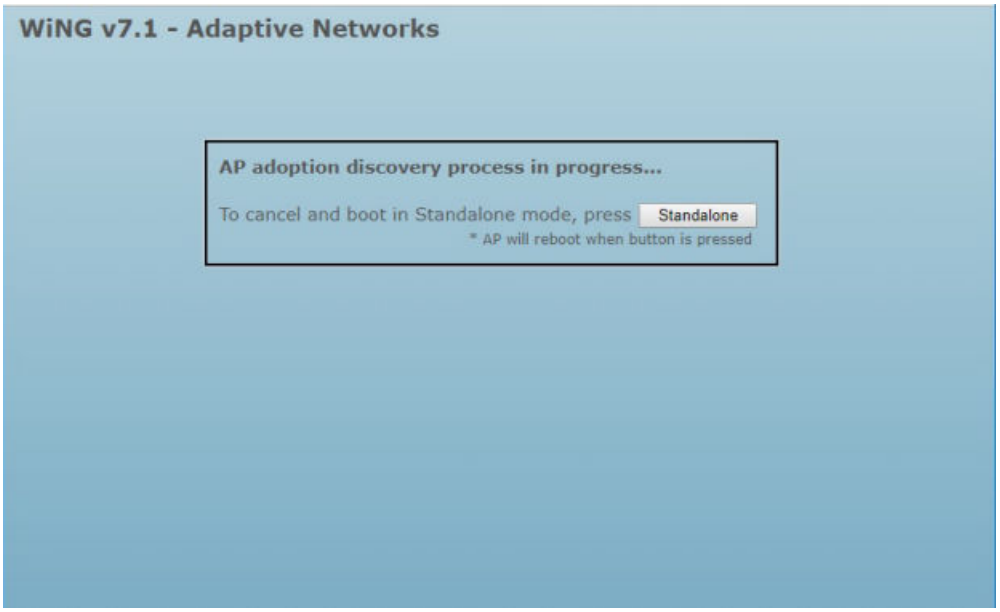
Secondary IP address - This is the ZEROCONF IP address '169.254. xx.yy'. Where, '`xx`' and '`yy`' are the last two octets of the AP's MAC address in decimal format. Note, the AP's MAC address will be printed on the box.

For example:

If AP's MAC address is: *00:C0:23:00:**F0:0A***

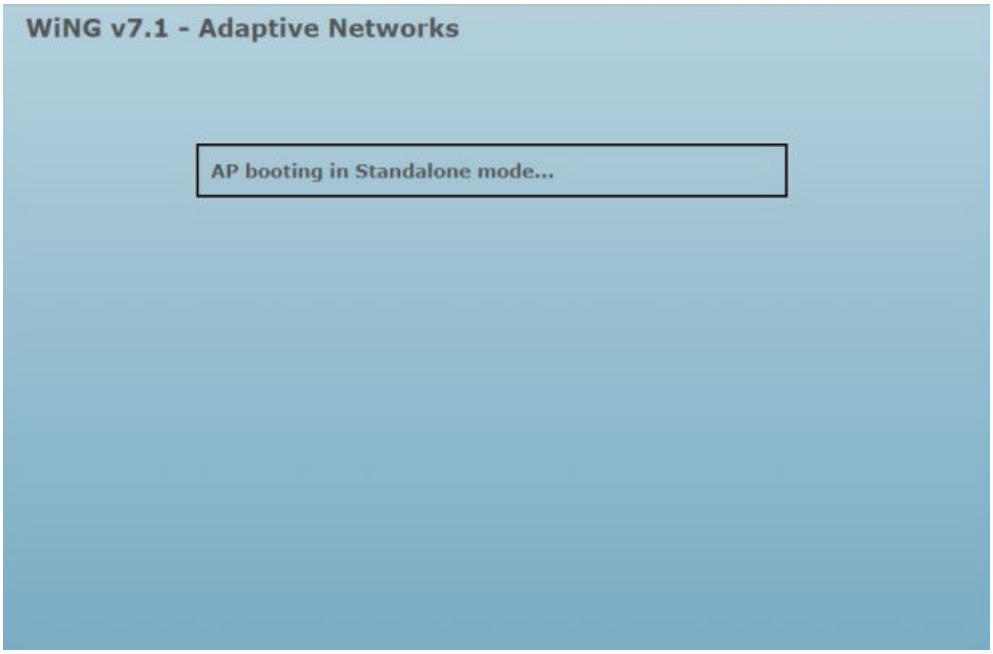
The secondary IP address will be: *169.254.**240.10***

You will be presented with the following screen:



2 Click the **Standalone** button to move into the `Standalone/WiNG` mode.

The following screen displays:




3 After the AP has rebooted, use the following default credentials to login:

username: `admin`

password: `admin123`

## Resetting an AP's Mode of Operation

This section describes how to reset an adopted or standalone AP's mode of operation.

Once an AP's mode of operation is set to 'Centralized' or 'Distributed', and the AP is in the adopted state, you can reset the AP's mode of operation through the adopter.

For information on resetting the mode of operation of an AP adopted to WiNG VC/Controller or a Standalone AP, refer to Resetting Distributed AP's Mode of Operation on page 1127.

For information on AP adopted to ExtremeCloud Appliance, please refer to the ExtremeCloud Appliance User Guide available at https://extremenetworks.com/documentation.

*Resetting Distributed AP's Mode of Operation*

**Resetting mode of operation of an AP adopted to WiNG VC or WiNG Controller**

To revert an AP5XX, adopted to a WiNG VC or WiNG Controller, to factory-default mode of operation (that is, mode not specified) issue the following command on the WiNG VC/Controller:

```
#factory-reset deep <AP-HOSTNAME>
```

Note
The <AP-HOSTNAME> parameter represents the host name of the AP on which the command is to be implemented.

The AP's adoption status is lost, it reboots immediately with its mode of operation not specified.

**Resetting a standalone AP's mode of operation**

To reset a standalone AP to the 'Centralized' mode, on the AP, issue the following command:

```
#operational-mode centralized
#reload
```

Or

Follow the steps below to reset the AP to factory-default mode of operation (that is, mode not specified).

1 Access the AP's console.
2 Enter the following login credentials:

| | |
|---|---|
| username | `resetDeep` (with 'D' in upper case) |
| password | `FactoryDefaultDeep` (with 'F', 'D' and 'D' in upper case) |

Note
The AP reboots in the temporary 'Centralized' mode.

*Resetting Centralized AP's Mode of Operation*

This section describes how to revert the mode of operation of an AP operating in the 'Centralized' mode.

If the AP boots up in the 'Centralized' mode, use the following command to reset the mode of operation to factory-default setting (that is, not specified). Issue the command on the AP.

```
#cset factoryDefault deep
```

When you issue the above command, the AP reboots and moves into the discovery mode, where it tries to discover its mode of operation.

To reset the mode of operation to *Distributed*, issue the following command in the AP's configuration context:

```
#cset personality distributed
```

The AP to controller adoption is lost, the AP reboots and moves into adopter discovery mode.

# Glossary

**ad hoc mode**

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

**ARP**

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

**ATM**

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

**BSS**

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

**Chalet**

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

**CHAP**

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

**CLI**

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

**Data Center Connect**

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

**DoS attack**

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable

from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

### DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

### EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

### ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

### Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

### Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond

ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

### ExtremeCloud Appliance

The ExtremeCloud Appliance, the newest addition to the Smart OmniEdge portfolio, is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge. Learn more about ExtremeCloud Appliance at https://www.extremenetworks.com/product/extremecloud-appliance/.

### ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

### ExtremeControl

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at https://www.extremenetworks.com/product/extremecontrol/.

### ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: Modular (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); Stackable (X-series and A, B, C, and 7100 series switches); Standalone (SSA, X430, and D, 200, 800, and ISW series); and Mobile Backhaul (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

### ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

**ExtremeXOS**

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

**FHSS**

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

**IBSS**

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

**MIC**

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

**netmask**

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

**PEAP**

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

**SSL**

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

**syslog**

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system

implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)